# Energy Theft Strategic Threat Assessment & RAS and ETU Case Acceptance Criteria

**Purpose**

The Police led Energy Theft Unit (ETU) is a partnership between REC and the City of London Police as detailed in REC Schedule 7, section 9. It will operate independently, however its strategic priorities will be agreed by the REC and updated as required during the term of the Sponsored Agreement.

This Energy Theft Strategic Threat Assessment should outline industry specific threats, focusing on risks, vulnerabilities and organised crime targets which will guide the ETU's priorities and the referral criteria and scoring.

The Referral Assessment Service (RAS) as detailed in REC Schedule 7, section 10 and Annex 4, will receive and triage referrals from REC parties and those that meet the required criteria will be progressed to the ETU. The RAS and ETU Case Acceptance Criteria and scoring matrix will reflect the key threats surrounding Energy Theft identified by the Energy Theft Strategic Threat Assessment as pertinent to both REC Parties and Energy Consumers.

The scoring matrix will take into account the level of threat, harm or risk identified as well as vulnerability issues and links to organised crime and professional enablers of Energy Theft. It will also consider the opportunities for positive, alternative means to resolve cases of Energy Theft referrals where a protracted investigation may not be beneficial or appropriate, such as social media account take downs, account freezing orders, cease and desist orders or organisational and industry learning points to prevent similar types of Energy Theft from occurring.

Each case of Energy Theft referred is to be assessed individually using the Case Acceptance Criteria and scoring matrix to determine if it should be accepted or referred back to the referring REC Party with feedback. The RAS may make requests for additional information, if available, to inform the assessment before the scoring can be completed.

If a case is rejected but the referring REC Party believes this to be incorrect then an escalation and appeal process may be followed.

The Case Acceptance Criteria and scoring matrix is designed to reduce subjectivity to ensure a consistent and transparent assessment of Energy Theft case referrals.

The cases taken on by the ETU should reflect the current Energy Theft threat as defined by this document and any emerging threats determined by tactical analysis. In the case of emerging threats, the ETU may accept cases of Energy Theft that sit outside the Energy Theft Strategic Threat Assessment and Case Acceptance Criteria where appropriate in the circumstances. This includes self-generated referrals resulting from intelligence or other information provided to the Energy Theft Unit based on their professional judgement and that the Head of the Energy Theft Unit reasonably believes to be in the interests of REC Parties and Energy Consumers.

**Energy Theft Strategic Threat Assessment**

A. Organised online groups offering a "Meter Replacement Service" for a fee

   Most groups promoting Energy Theft organise their services and discourse through Telegram, using other social media platforms to advertise their ideologies and their Telegram group. Some do maintain an online presence elsewhere e.g. Facebook, X, Instagram, TikTok, though the

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

interaction and discussions on these platforms are extremely limited compared to Telegram. Many of the groups also make use of influencers on social media to advertise their groups with the majority of these on alt-right sites such as BitChute and Rumble. They promote the false concept that energy is already paid for via taxes and that by removing the legitimate Supplier registered meter and replacing it for one privately purchased the occupier will no longer be required to pay for their energy consumption.

The ideologies promoted by the groups often align with Sovereign Citizen or Freeman of the Land and can often be linked to other fringe movements and conspiracy theories. Regardless of the rationale for replacing the meter provided by the groups online, the fundamental driver or motivating force behind the groups appears to be financial gain, with each of these groups charging for their services. Charging £450 per meter replacement, and with the larger groups having over 19,000 members the potential income from replacing meters is in the millions. There are also additional income streams from group meetings (online and for some group leaders in person) and 1-2-1s for advice which are normally charged at between £50 and £100 to attend. Some groups may also promote and sell other products linked to their ideology such as water filters, homeopathic treatments and also home security items to prevent entry to organisations, such as energy companies. There is also no indication this income is declared for tax purposes.

The common process these groups follow and promote is:

1. Replace the properties existing meters, “smart” or otherwise with their “own” that they control, to avoid having utilities cut off remotely. Groups do not believe suppliers can shut off supply unless they dig into the ground. The major groups advertise “qualified engineers” who can swap out meters, ranging from £250-£450 depending on group and region.

2. The occupant tells their supplier they have ‘moved out’ of their property, to end their “contract” with a supplier. Some groups label this as their “legal fiction” moving out, either way individuals should know at this stage that what they are doing isn’t completely legal.

3. The individual then stops paying bills, whilst maintaining occupancy in the residence they “moved out” from. Some groups suggest sending letters to the occupant’s original energy supplier regarding the continued use of the utilities and/or the denial of payment for the property’s utilities. The groups will provide templates in some instances free but often paid for, with advice and guidance on how to fill it in. Others advise a “no contact” policy.

4. The individual then secures their property. Some groups recommend high end locks on all entrances (e.g., doors, windows). Often groups recommend obtaining a “vulnerable person” status, to avoid unwanted parties entering their property (i.e., bailiffs and associates of utility companies). Most groups recommend securing outside meters, for example with metal boxes and bolts.

5. Groups provide guidance on what to do when confronted (e.g., by bailiffs or representatives of suppliers). Videos of these confrontations are posted for people to replicate. Most recommend avoiding contact as a priority (i.e. do not answer door or respond to letters). If the individual has obtained vulnerable person status, they are to say the bailiff/engineer cannot enter, even when presented with a warrant. When avoidance is not possible or wanted, some groups recommend “legislation” to quote.

This email/document and its contents have been classified as ‘Internal & Partners’ by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

6. If step 5 fails and meters are either replaced with Supplier controlled meters or removed and the supply left disconnected at the cut out/ECV, the group recommend simply replacing them again using the group's services (at a cost) and starting the process again.

The threat with this activity is that unauthorised and unknown individuals are entering consumers homes and businesses and carrying out metering work without the required accreditation and fitting meters of an unknown quality. Poor quality connections and/or meters can lead to electric shocks, fire, gas leaks and explosions. Due to the way it is promoted and sold online, often targeting and appealing to vulnerable households looking for an easy solution to rising costs, this is a growing threat rapidly increasing in scale that needs to be addressed.

B. Professional Enablers – Tradespeople offering "tampering as a service"

Tradespeople, whilst engaged in legitimate business and services may offer additional illegal services, for a fee, such as tampering with a meter to enable it to under record or to make an illegal connection direct to the Network bypassing the metering equipment. This may be offered as a stand alone service via word of mouth or social media but also often whilst onsite completing legitimate work e.g. carry out work to fit a new kitchen, offer to connect the new wiring for the kitchen direct to the mains, similar for hot tubs, electric showers and EV chargers. This may also occur when gas work is carried out, an offer is made to tamper with the gas meter whilst a boiler service is carried out. They may also imply this is not illegal to the consumer by phrasing it as an "upgrade" to the meter to help reduce your bills or similar terminology. As they attend multiple addresses across multiple suppliers it is difficult for a single supplier to identify and tackle these individuals who may be facilitating and profiting from energy theft at a large scale. There is also the safety implications or high load appliances being connected to the Network without the required service upgrades or checks.

C. Rouge Landlords/Developers – committing or facilitating Energy Theft over multiple properties and developments

Developers or their contractors may choose to connect multiple new build properties or developments where existing properties are split into multiple units, to the Network to gain a utility service illegally. They may make the connection, fit a privately purchased meter and then sell or rent out the properties on without any official meter point registration or supplier. They may alternatively opt for an official service to be installed and registered but still fit a privately purchased unregistered meter instead of organising or waiting for a supplier to install and connect a meter. This may be because of the certification required to ensure that the wiring/pipe work is up to standard before a Supplier will fit a meter is not available.

Landlords who rent out HMOs or properties where rent in inclusive or utility bills may also be committing Energy Theft in multiple properties. The tenants are paying for energy costs via their rent but the Landlord is not paying the utility bills and are pocketing the money.

The motivation behind this is often financial, they can have a service or meter installed illegally for a lower cost or more quickly than having it installed legitimately. Where HMO or rent inclusive of bills is concerned it means the landlord has no or lower energy costs to maximise their profits. It may also be to avoid detection of other issues such as lack of planning or substandard work on internal wiring etc.

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

Whilst the landlords or developer profit, the unsuspecting new owners will be left with an illegal and often substandard or dangerous connection which they will need to resolve, often at their own costs and tenants may unwittingly be put at risk with a dangerous supply installation or tampered meter in their home.

D. Cannabis Cultivation – Electricity Theft to supply grow houses/buildings

The cultivation of cannabis uses a large amount of electricity to power the lamps, watering systems and ventilation. The electricity meter is normally bypassed to avoid high electricity bills which would reduce the profit, but also to avoid detection as the increase in consumption would indicate suspicious activity at the property. The organised crime groups involved in cannabis cultivation are also often involved in other types of criminal activity such as modern day slavery, cuckooing, people trafficking, drug distribution, often via county lines, and may also be linked to violent crime involving weapons. The high load plus the sometimes haphazard nature of connections made illegally to the network can lead to a significant risk of network overload, electrocution and fires and properties are often booby trapped increasing risks to those who may attend. These cultivations are often carried out in rented properties in residential areas, exposing the neighbouring properties and residents to risk as well as damage to the property they have rented and adapted for cannabis cultivation. Whilst cannabis factories are often investigated by the police the electricity abstraction may not be the focus of any investigation or be included in any criminal charges so may not be reflected in crime figures. By increasing the focus on how the electricity abstraction is carried out and who is carrying out the work and any similarities between individual instances, it may lead to greater understanding of links between different cultivation sites.

E. Cryptocurrency Mining – Electricity Theft to supply computer and cooling equipment

Whilst cryptocurrency mining is not a crime it is an electricity intensive activity requiring a large volume of computing equipment and cooling equipment, to be profitable the organisations involved may opt to bypass the meter to prevent high electricity bills. Similar to cannabis factories, organisations who commit Energy Theft to facilitate cryptocurrency mining may be involved in other criminal activity.

F. Individuals who repeatedly offend – Engagement, intervention, support and education unable to deter or prevent repeated instances of Energy Theft

Individuals who commit Energy Theft in their own home or business are not seen as a strategic threat and are expected to be resolved by REC Parties. An individual may continue to interfere with the metering installation and/or the connections to the Network in spite of numerous interventions, replacement meters, disconnections or where disconnection is not possible. If reporting the incidents to the regional police force has not been successful in the prevention of reoccurrences then a referral to this service may provide a pathway for appropriate enforcement action utilising the expertise on Energy Theft from this unit.

**Case Acceptance Criteria**

1. Seriousness of the Energy Theft
    - Threats identified in the Energy Theft Strategic Threat Assessment
    - City of London Police's National Lead Force Priorities

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

    - Bring offenders to justice and disrupt organised crime.
    - Identify and divert individuals at risk of offending or reoffending.
    - Reduce harm and prevent victimisation.
  - PIP Level – an assessment of the overall complexity of the referral, Investigation Introduction (College of Policing)

2. Evidential Assessment
   - Age of the offending – when did the offence occur?
   - Evidence of offending – allegation supported by available/obtainable evidence?

3. Offender Assessment
   - Named Suspect – has the suspect been identified already?
   - Scale – single suspect in own property, single suspect over multiple properties, professional enabler offering a service, or organised crime group, etc.
   - Links to other criminal activity

4. Victim Assessment
   - Type – Energy Suppliers/Network Operators, members of the public, vulnerable persons, etc.
   - Community impact
   - Number of victims

5. Harm/impact to Victims
   - Public Risk:
     - Ongoing risk to the public, e.g. dangerous tamper in situ in a business open to the public, block of flats or other at risk situation. Multiple repeat offender who will reoffend immediately with no regard for safety of self or others.
     - Significant potential risk, e.g. Individual or group offered tampering as a service to multiple individuals and likely to reoccur.
     - Low potential risk e.g. repeat offender in a single premises who continues to tamper regardless of previous action and warnings.
     - No risk to the public – no ongoing tampering, previous tampering has been resolved, only loss was financial and unlikely to reoccur
   - Financial gain or loss – volume and value of stolen/abstracted kWh as well as financial gain from use of stolen energy e.g. cannabis cultivations, bit coin mining, tanning salons etc. Also financial gain from professional enablers selling a service or device to facilitate Energy Theft.
   - ☐ Reputations Damage – for both referring party and the City of London Police. Is there likely to be serious reputational damage if action is not taken/is taken.
6. Marketing and Provision of Unauthorised Work to Facilitate Energy Theft
   - Advertising and charging for the installation of unauthorised and undocumented gas and electricity services from the main network to a property.
   - Advertising and charging for a meter replacement or removal with the false claim that the consumer will no longer have to pay energy bills.
   - Providing meter tampering as a service

**Scoring Matrix**

The RAS will utilise the scoring matrix provided by the ETU to assess the referral and determine if the case should be referred on to the ETU. The RAS may contact the SPOC, Case Handler or Field

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

Investigator detailed in the referral if additional information is required to complete the assessment or if they believe additional information, if available, may strengthen the referral.

If a referral is accepted by the RAS and referred on to the ETU they may accept the RAS recommendation or they may reject the referral.

**Escalation Process**

If following the assessment and rejection of a referral the REC Parties nominated Specified Point of Contact (SPOC) requests a review of the decision they will need to upload a Referral Decision Review Request Form (appendix 1) to the RAS via the designated file transfer mechanism. This will need to detail the rational for the appeal, examples are additional evidence availability, media opportunity identified, wider industry impact or any other special circumstances to be considered.

The initial referral and the referral decision review request will be reviewed via a panel consisting of a representative from the ETU, the RAS Manager and an Energy Theft Subject Matter Expert nominated by RECCo. This panel will be convened to discuss the merits of the referral with the ETU representative making the final decision. The REC Parties SPOC and Investigator/case handler may also be invited to attend the meeting or part of the meeting to explain their rationale and answer any questions. Following this meeting the REC Parties SPOC will be informed of the final decision regarding the referral. This process should take no longer than 10 working days unless there are extenuating circumstances where additional investigation, data or information is required before a final decision can be made.

**Appendix 1**

| Section | Field Name | Referral Detail | Description of information or detail required | M/C/O |
|---|---|---|---|---|

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

| | | | | |
|---|---|---|---|---|
| **Referrers Details** | Party ID | | RECCo Party Name & MPID or Short Code | M |
| | Investigation ID Number | | The investigation ID of the referral that the Decision Review Request is being made | M |
| | Date of Referral to RAS/ETU | | Standardised date format - ddmmyyyy- of case that is being request for review initialy upload to SFTP or REC Portal | M |
| | DAte of Decision Reveiw Request | | Standardised date format - ddmmyyyy- of Decision Review Request upload to SFTP or REC Portal - | M |
| | Party SPOC Name | | If no one individual, please enter Team Name | M |
| | Party SPOC Telephone No. | | Individual or team number | M |

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.

| | | | | |
|---|---|---|---|---|
| | Party SPOC Email address | | Individual or group email account | M |
| | Case Handlers Name | | If different to SPOC | O |
| | Case Handlers Telephone No. | | If different to SPOC | O |
| | Case Handlers Email address | | If different to SPOC | O |
| **Decision Review Request** | Rational for Review Request | | detail the rational for the appeal, examples are additional evidence availability, media opportunity identified, wider industry impact or any other special circumstances to be considered. | M |

This email/document and its contents have been classified as 'Internal & Partners' by RECCo. This data should be handled in line with RECCo data handling requirements. If you have received this data in error, please advise the sender or author and delete the data.