

Review of Energy Theft Processes

31 October 2023
Version 1.0

Contents

1 Background 3
2 Purpose 3
3 Executive Summary 4
4 Overview of the end-to-end Energy Theft process 6
5 Applicable licence and code requirements 8
6 Supplementary analysis of Fire and Police service reporting data 9
7 Engagement with industry participants 13
8 Gap analysis summary 17
8.1 TDIS participation 17
8.2 Evidence collection, retention and access 19
8.3 Monitoring and reporting gaps 20
8.4 Monitoring of sites with new connections & those post Energy Theft resolution 21
8.5 Police prosecutions 22
8.6 Reporting losses into settlement 23
8.7 Objection to a change of supplier request 24
9 Recommendations summary 26
9.1 Awareness / Incentive 26
9.2 Monitoring / reporting 26
9.3 Obligation / Responsibility 27
10 Next Steps 28
11 Appendix 29
11.1 Appendix 1: Process maps 29
11.2 Appendix 2: Reference log documents 33
11.3 Appendix 3: Selected workshop verbatim comments 34
11.4 Appendix 4: Gap and reference log 35

1 BACKGROUND

Energy Theft has long been a problem within the industry, with the recent Theft Estimation Model (TEM) valuing it at between £600m and £1.4bn annually[1]. Whilst there are licence obligations on Energy Suppliers and established resources in place to investigate and prevent Energy Theft, it remains a challenge for Market Participants to identify and report instances of Energy Theft. Current processes still largely rely on outdated procedures and techniques to detect theft, which do not reflect the modern Energy Theft techniques used today, such as the use of machine learning to identify trends.

RECCo initiated a project to complete end to end (E2E) process mapping to document the key actors and steps they take in relation to energy theft detection and prevention. This project identified a number of potential opportunities to use data to tackle Energy Theft on a larger scale. By producing process maps and conducting a SIPOC analysis[2], formulating a reference log alongside data analysis and facilitating industry workshops, Energy Theft can be addressed through multiple aspects.

2 PURPOSE

Acknowledging the challenges being faced within the industry, and the large value range of Energy Theft, RECCo would like to explore the opportunities to improve the theft end to end processes and analyse any gaps in the process to improve: the detection, reporting, prevention, and awareness of Energy Theft; also ensuring a sufficient deterrent is in place. The high-level scope of the work is outlined below:

- provide a comprehensive overview of end-to-end industry processes
- identify applicable current licence and code requirements
- identify areas of low industry awareness and understanding of processes
- identify any gaps in the E2E process where no REC Party has a clear role and responsibility
- identify gaps in current industry monitoring and reporting

This report sets out answers to these questions in the following structure

- Process
- Findings
- Outcomes

There is also a section highlighting recommended next steps.

[1] See: https://www.retailenergycode.co.uk/fs/wp-content/uploads/2023/01/TEM-report.pdf

[2] Suppliers, Inputs, Processes, Outputs, Customers (SIPOC) – a tool for documenting business processes from beginning to end

3 EXECUTIVE SUMMARY

The process maps were created based on the overall lifecycle of an energy supply as highlighted below.



The process maps capture the key areas that can give rise to Energy Theft and document the steps, actors and obligations in relation to Energy Theft that apply to each party. These were used as a tool to identify any gaps within the process that can give rise to Energy Theft or enable Energy Theft to go un-noticed.

The gaps drawn out and highlighted by parties throughout the project covered the following areas

- Awareness / Incentive
- Monitoring / Reporting
- Obligation / Responsibility

Whilst the gaps identified are not new, collectively they represent known issues that have existed for some time. Individually the gaps are not likely to contribute to a significant volume of Energy Theft, collectively they are likely to, with some gaps directly impacting others within the process.

A summary of the gaps is provided, by area, below.

Awareness / Incentive

Broadly parties are aware of how the processes work, however, there are some grey areas that would benefit from clarification.

Existing incentives are not as effective as they are designed to be with some suppliers not engaging fully with industry wide schemes such as the Theft Detection Incentive Scheme (TDIS).

There is also scope to review and explore the use of incentives elsewhere in the lifecycle (for example entering unrecorded volumes into settlement) to encourage appropriate behaviours.

Monitoring / Reporting

There is an overall lack of consistency in the approach taken by parties to monitor aspects of the process, specifically new connections, unregistered sites and those where a supply has been interrupted due to Energy Theft.

There is also a lack of central reporting and a single view outside of the TDIS for sharing information within the industry relating to the volume and detail of investigations and their outcomes. This can make it challenging for parties to act in a co-ordinated manner, especially where there are multiple supply parties with an interest in a particular theft case.

Obligation / Responsibility

Parties are aware of their obligations and responsibilities in relation to Energy Theft, however, there are some Suppliers and Network Parties that are not consistently adhering to them particularly those relating to proactive theft detection practices.

There is also scope for changes to some of the existing obligations (for example change of supplier) to assist with the prevention of Energy Theft.

Conclusion

This project has re-affirmed how complex the issue of Energy Theft is and whilst it is likely that no individual gap contributes a significant volume of theft, collectively they do. There are a number of improvements that can be implemented, some more complex than others and whilst not solving the problem of Energy Theft, by improving working practices, collaboration and resources available, parties' will be able to detect and resolve theft earlier. This would reduce the overall cost and potential safety impact to Consumers.

Recommendations

Multiple recommendations have been made and are detailed further in the report (here) with a summary of the key themes below.

- Review of the existing incentive scheme to determine if it remains suitable to encourage the desired behaviours in relation to Energy Theft and if additional incentives are required elsewhere in the process.
- Review and publication of Best Practice guidance documentation to improve awareness of, but not limited to, the following topics:
    - Collection, retention and access to evidence obtained during Energy Theft investigations.
    - Responsibilities of Network Parties and Suppliers when encountering an unregistered site
    - When it may be appropriate to pursue a prosecution for Energy Theft
- Review of reporting and monitoring requirements to ensure parties are conducting their responsibilities as they are designed and intended.
- Utilising data that is currently available (e.g., TDIS data) to improve accuracy of reporting and provide further insight into persons committing Energy Theft.
- Provide clarification of the wording of existing regulation to remove ambiguity and assist with compliance.

Whilst this report identifies multiple gaps across the energy supply lifecycle and provides recommendations to address some of these, it is not exhaustive. As new technologies, products,

services and ways of working develop, new gaps are likely to occur with new methods of tackling these required. As such RECCo should consider how it should approach this.

4 OVERVIEW OF THE END-TO-END ENERGY THEFT PROCESS

Process

In order to understand and identify any potential gaps within the process that could contribute to Energy Theft, process maps were created setting out key stages across the energy supply lifecycle. The energy supply life cycle was chosen as opposed to the Energy Theft lifecycle (as outlined at the ASE (Accelerated Solutions Event) in 2022)[3] as it has stronger potential to draw out gaps and failures in existing processes. This approach considers the pro-active aspect of theft detection and prevention that leads to suspicion of Energy Theft, whereas the theft lifecycle tends to be reliant on suspicion already being there.

The process maps built on the work completed at the ASE and incorporated information provided by parties via other forums such as the Energy Theft Reduction Expert Group (ETREG), theft forums and the TDIS. The lifecycle is set out below.



Across the lifecycle a total of nine process maps have been created, as listed below. The process maps can be viewed in Appendix 1.

Provision of Network Infrastructure

- Provision of Network Infrastructure

Meter Installation and Registration

- New Connection
- Unregistered site (no supplier appointed)

Supply of Energy

- Meter reading / Smart alert received

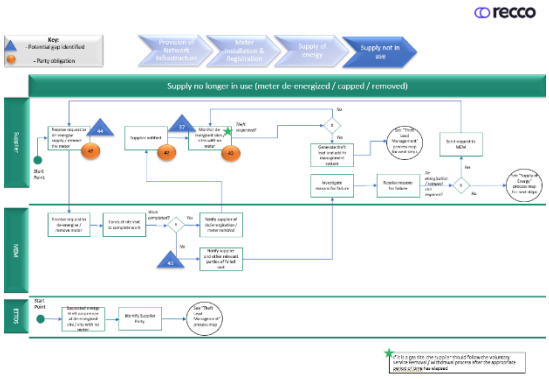


Figure 1: Supply no longer in use (meter de-energised / capped / removed)

[3] See: https://www.retailenergycode.co.uk/bringing-the-industry-together-to-re-energise-the-fight-against-energy-theft/

- Theft Lead Management (Supplier)
- Theft Lead Management (Network Party)
- Engage in Theft Detection Incentive Scheme

Supply no longer in use

- Supply no longer in use (meter de-energised / capped / removed)
- Supply no longer in use (Service removal)

The steps within the process maps have been captured at a high level to document the key activities involved. The intent of the process maps is not to reflect at a low level the different variations of activities and actions taken by different parties, but to demonstrate the end to end process enabling the critical gaps and differences to be identified (rather than low level differences that may not have any significant impact on the identification or assessment of theft). However, it is acknowledged that there are a minor number of lower level steps that are critical to the success, such as the different approaches to desktop analysis, and these have been called out as potential gaps.

Obligations placed on parties via their respective licences or industry codes have been mapped to the relevant step as have gaps in the process. The gaps have been categorised into the following areas:

- Awareness / Incentive
- Monitoring / Reporting
- Obligation / Responsibility

A detailed breakdown of the identified obligations and gaps has been included in the "*Gap analysis*" section of this document.

A detailed list of the gaps has been included in Appendix 4.

Findings

The initial drafting of the process maps was validated by the REC Theft SME team and with industry participants via two virtual workshops (see "Engagement with Industry Participants" section). Subsequent feedback has been provided with the process maps being revised accordingly.

The updated versions of the process maps were issued to industry participants to provide a further opportunity to comment and highlight any gaps. The document was issued on 11th August for a two-week period, with parties invited to provide feedback via the REC Technical



Services team. A further version was issued to ETREG members for review in September with feedback being incorporated into the final version.

Output

An artefact has been produced documenting each of the process maps, the obligations and gaps identified within the process. The artefact includes links to make it easily navigable by users to understand their obligations within the process. See Appendix 1

5 APPLICABLE LICENCE AND CODE REQUIREMENTS

Process

A reference log has been recreated that captures relevant licence conditions and energy code obligations that are associated with Energy Theft, focusing on those obligations that are applicable to Energy Suppliers and Network Operators (but not limited to only these parties).

The Ofgem and RECCo websites and documents were used to identify the obligations and licence conditions relevant to the process maps. The log also includes DCUSA and SPAA obligations for reference to ensure previous obligations were also included in the REC schedules.

See Appendix 2 for a list of the documents used.

Findings

The volume of obligations placed on Network Parties and Energy Supplier, in relation to those on other parties, supports the position that Network Parties and Energy Suppliers can have significant impact, influence and responsibility in managing Energy Theft.

The volume of obligations is high and, as a result, they cover multiple aspects of Energy Theft across the end to end process. Although there are extensive obligations for parties to meet, some gaps have been identified that could be mitigated through the introduction of new obligations or revisions to existing obligations that reduce / remove ambiguity and provide clarity to parties. This would reduce the likelihood of different interpretations of the same obligation. In addition, further opportunities lie in improving the awareness parties have of these obligations.

Insights from the two workshops, held with experts from the energy industry, alluded to the notion that many parties are not aware of what obligations exist, therefore creating gaps in knowledge around which obligations need adhering to. This can lead to compounded errors within the end-to-end Energy Theft lifecycle with parties not being clear on how an obligation placed on them impacts another party elsewhere in the lifecycle. This can be attributed to the obligations being spread across multiple codes of practice and licence conditions. For example, a Supplier may have an obligation within the REC which could impact a network party obligation under the UNC which the supplier may not be aware of.

The awareness around these obligations could be improved by providing increased communication on cross party obligations for example through a user guide that brings together



all code and licence obligations in relation to Energy Theft, which party they apply to and how they link together.

Output

A reference log detailing the licence and obligations has been created. This has been linked to process maps produced alongside this report. See Appendix 4.

6 SUPPLEMENTARY ANALYSIS OF FIRE AND POLICE SERVICE REPORTING DATA

Process

Prior to the project commencing, RECCo submitted a Freedom of Information (FOI) request to obtain data from national fire and police services; to understand both the volume of police action taken in relation to Energy Theft and the health and safety impact of Energy Theft.

Data was received from the services across Great Britain, which has been analysed to provide insight to determine if any meaningful trends can be identified. It should be noted that 23 of the police forces (over 50%) did not or were unable to provide a response to the FOI and of those who did, many advised of limitations in the data due to how energy theft is recorded in their systems.

The data included in the analysis has been taken from Leicestershire, Bedfordshire, Cambridgeshire, Devon & Cornwall, Dorset and Hertfordshire.

Findings

Leicestershire, Bedfordshire and Dorset will be compared for Outcome of Investigations. However, only Leicestershire and Bedfordshire will be compared for number of reports for 2021/2022 due to the information being unavailable for Dorset.

Cambridgeshire, Devon & Cornwall and Hertfordshire will be compared for Number of Reports in 2020/2021. However, only Cambridgeshire has provided the Number of Charges as a result of those Reports.

This analysis investigates whether there is any correlation between Reported Energy Theft, the location of Energy Theft and the outcome of Investigations into Energy Theft.

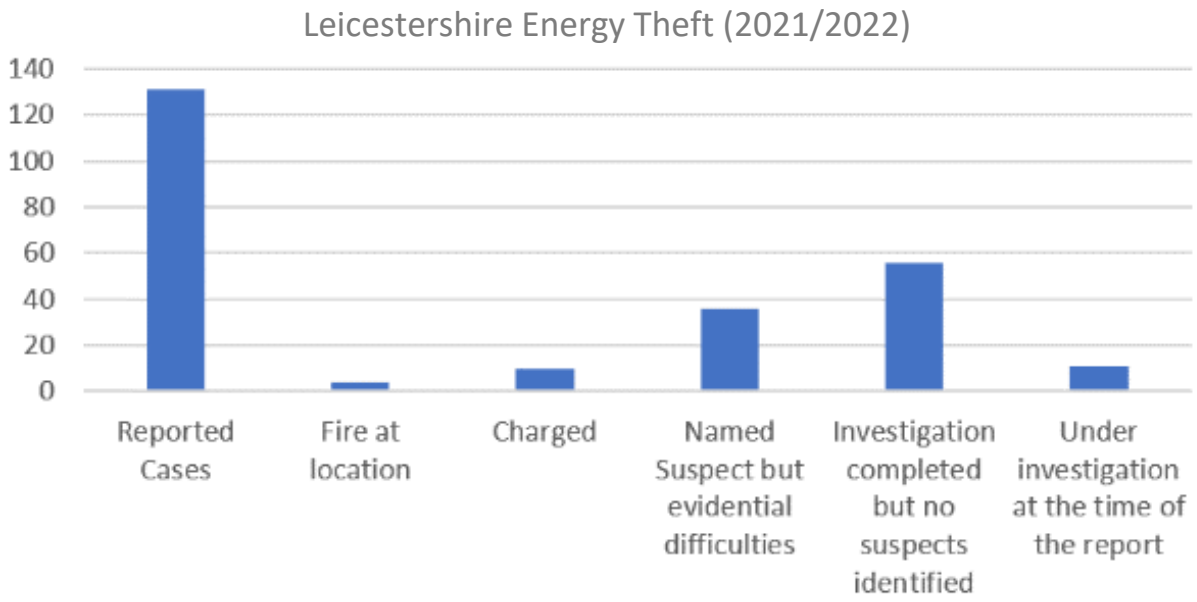
Due to limited amounts of information, only Leicestershire, Bedfordshire & Dorset were comparable by year for 2021/2022. Moreover, Cambridgeshire, Devon & Cornwall & Hertfordshire were comparable by year for 2020/2021.

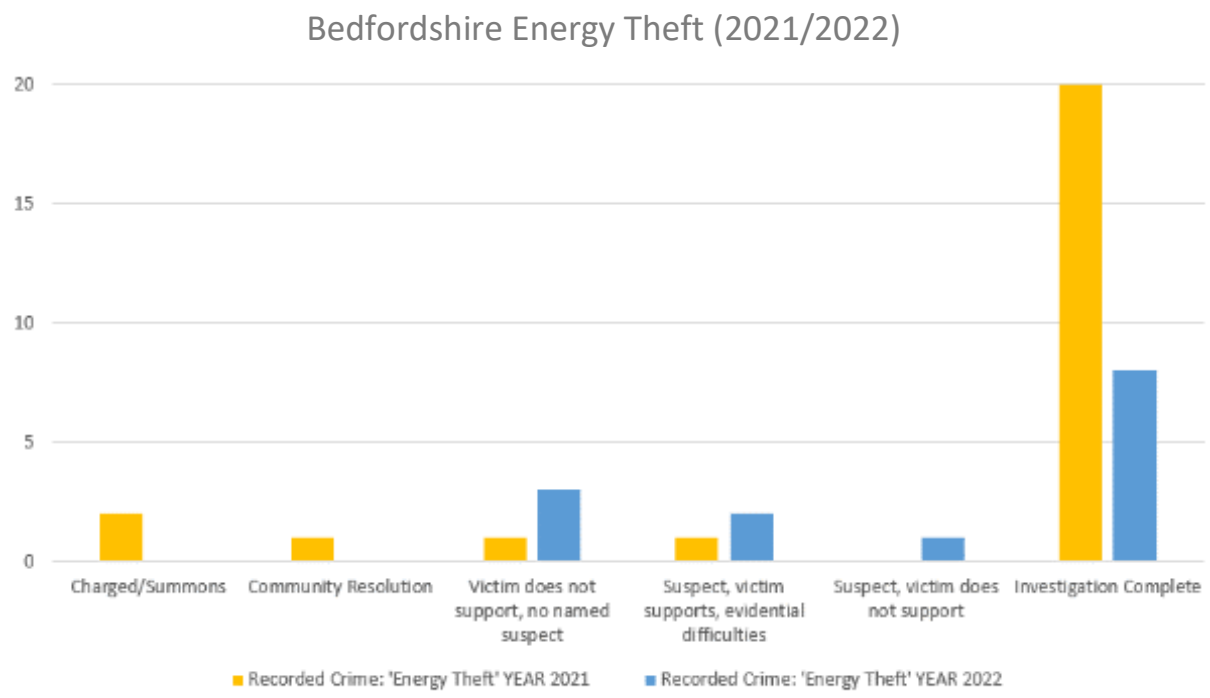
Challenges were faced during this analysis due to a limitation on available statistics, for example, Devon and Cornwall did not provide their charge rate for Energy Theft Crimes, only the report numbers. Therefore, little comparison could be made between counties with limited information.

Overall, Leicestershire had the highest number of reported Energy Theft cases and the most prosecutions because of those reports in comparison to other counties. This could support the notion that urban areas see a higher number of investigations and reports in comparison to rural areas, or it may be that Energy Theft levels are just as high in rural areas but lack the processes and resources for investigation.

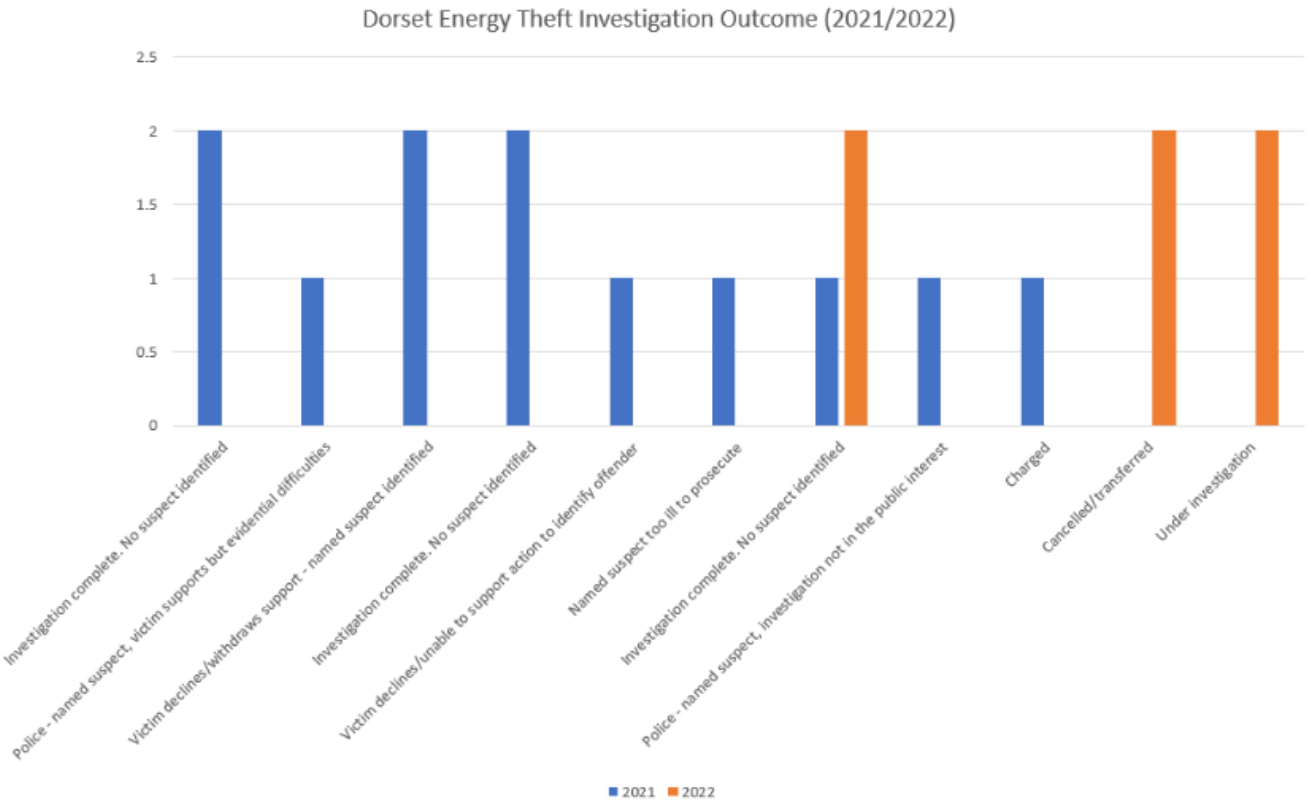
Leicestershire had 131 reported cases in 2021 and 2022, of which only 10 people were charged.

In comparison, Bedfordshire had 39 reported cases in 2021 and 2022, of which only 2 people were charged. The lower volumes, in comparison to Leicestershire, could be due to a lower Energy Theft crime rate, or due to a lack of reporting or follow up.

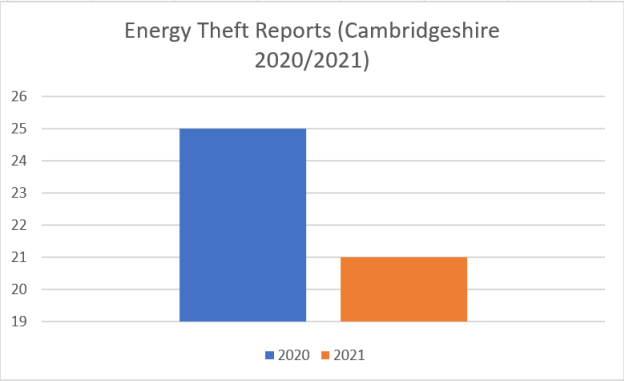


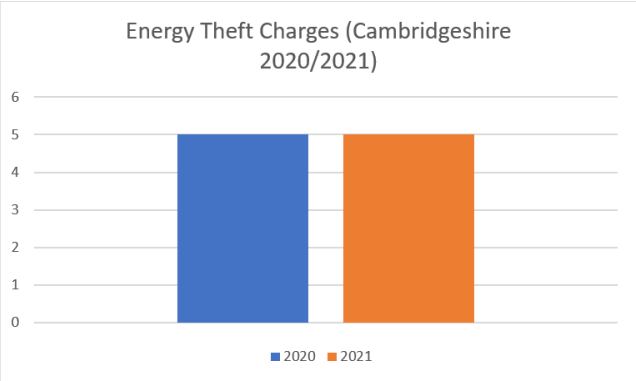


In Dorset, only 1 person was charged with Energy Theft in 2021/2022.



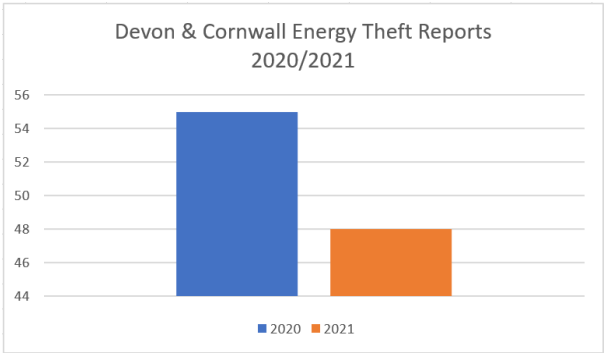
In Cambridgeshire during 2020/2021, there were 46 reported Energy Theft crimes and 10 charges for Energy Theft. It could be inferred that Cambridgeshire has established processes in place for Energy Theft crimes as their report to charge ratio is higher than other counties in England.

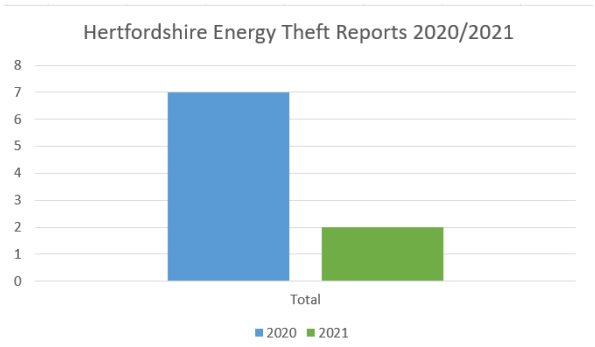




As for Devon and Cornwall, there were 103 reported Energy Theft crimes in 2020/2021. Due to limited information, this figure was not comparable to the amount of charges Devon and Cornwall Police made during 2020/2021.

Hertfordshire only had 9 reports of Energy Theft in 2020/2021 and 0 charges. It could be questioned as to why a large county such as Hertfordshire has a low report and charge rate in comparison to other counties of similar or smaller size analysed here.





Output

A detailed document containing supplementary analysis and commentary – see Appendix 4.

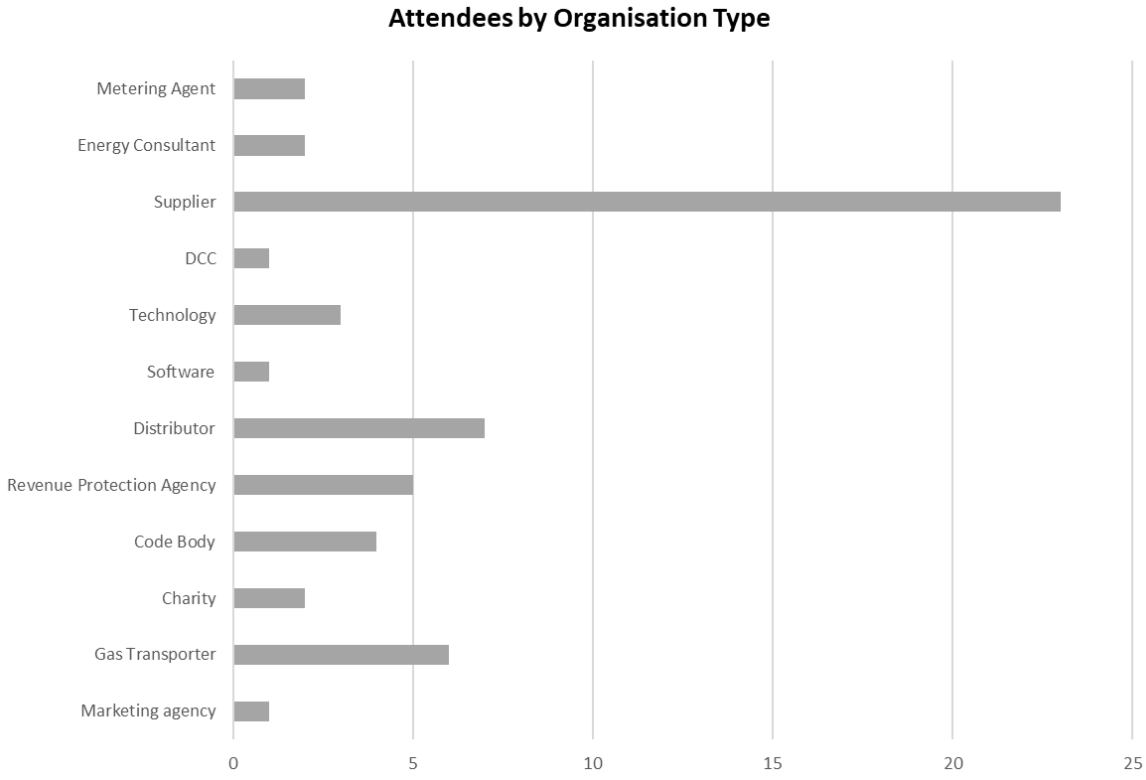
7 ENGAGEMENT WITH INDUSTRY PARTICIPANTS

Process

To enhance and enrich the process maps, two industry workshops were hosted. The objective of these workshops was to walkthrough each process map, validating the content and identifying any additional gaps within the process that could lead to Energy Theft going unnoticed, give rise to Energy Theft occurring or hamper efforts to detect and/or present Energy Theft.

The workshops were held on Monday 31 July 2023 and Tuesday 1 August 2023. Invited attendees were from those that had previously engaged with RECCo through multiple forums including the ASE events, Energy Theft Reduction Expert Group (ETREG), Energy Theft Forum, the UKRPA and known theft management process contacts. The invites included representation from parties across all aspects of the energy life cycle, alongside organisations such as Crime Stoppers and the various code managers/administrators. An open invitation was also published via the REC weekly bulletin. As part of this respondents were also invited to share their own theft management process maps.

Two workshops were chosen as this would allow attendees the choice and convenience to attend one day if they could not attend the other day. Each workshop lasted four hours, which allowed for introductions, instructions, analysis and discussion to take place. Attendees by organisation type are displayed below.



Of the process maps created, five were selected to be analysed during each of the workshops. These maps were:

- Theft Lead Management (Supplier)
- Theft Lead Management (Network Provider)
- Provision of Network Infrastructure
- Unregistered Sites and Consumers
- Engage in Theft Detection Incentive Scheme

These five maps were selected as they represented the processes that required actions/activity to be completed across the wider breadth of parties and/or had the highest levels of perceived gaps. The gaps covered the following areas:

- Awareness / Incentive
- Monitoring / Reporting
- Obligation / Responsibility

A live Whiteboard was used to facilitate the workshops in which the process maps and associated SIPOCs were presented. Participants were invited to review the content and provide any comments and gaps using colour coded post it notes representing each of the gap areas highlighted above. An example of the whiteboard is included below.



Once this exercise was completed for each of the maps and SIPOCs a deeper dive discussion was conducted to gain further insight and drill into the gaps.

Findings

Many insights were collected during the two workshops, which prompted further analysis into gaps alongside feedback on amendments to steps in the process. Some key insights are shown below focusing on issues / gaps identified. The process step updates have been incorporated into revised versions of the process maps:

Theft Lead Management (supplier)

- Suppliers are required to adopt shipper-less or unregistered sites where a meter is found, and gas or electricity is being consumed however some parties indicated this was not always the case.
- Data quality issues when submitting confirmed Energy Theft into central systems. For example, parties can enter an MPRN as free text which does not have validation applied before being submitted. Typos have been reported resulting in the MPRN being entered is invalid leading to a longer process for correction to the MPRN that matches the address.
- Money received from pre-payment customers (made in good faith) without a registered supplier does not always make its way back to the appropriate party instead it is shared as part of the un-allocated process.
- Not all parties are aware of or utilise no-notice warrants of entry.

Theft Lead Management (Network Party)

- Amendments to the process maps around theft in conveyance were suggested.
- Issues around an external party (e.g., property developer) installing a meter on a new MPRN before a supplier has been registered against the MPRN.
- There is a delay in Xoserve, in their role as the CDSP, being updated with incoming supplier information and Xoserve rejections not being followed up.
- Data quality and housekeeping of central systems causes issues for Network Parties when trying to report and allocate Energy Theft.

Provision of Network Infrastructure

Inconsistent approaches and lack of code guidance on when and how sites should be monitored to ensure new connections are registered with a supplier in a timely manner and have meter installations completed.

Unregistered sites and Consumers

- Suppliers and Network Parties may be wary of disconnecting a Consumer as they may incur reputational damage, or the affected party may be a vulnerable customer.
- Vulnerability assessments impact decision making and influence how an identified theft is treated in the future once it has been resolved and accurately reporting this.
- Network Parties have historically had issues identifying a MEM or tracing who originally installed a meter due to a lack of access to data.
- Customers are asked to contact the supplier of their choice to organise a contract, however customers struggle to organise a contract for shipper-less MPRNs as some suppliers are not aware of the process or refuse to take shipper-less MPRNs.



- Suppliers may lose track of the meter location or the consumer (this could be due to building development work) and use the "logical disconnection" flow within the disconnection process, to close off the MPAN when it actually remains on site and is now unbilled and un-registered.
- Suppliers claiming to have removed a particular meter (and sending the relevant D-flows stating this) in order to install and associate a different meter with the MPAN. However, they have not removed the meter and it remains on site. This is often encountered where an extra flat or business unit has been created but no MPAN exists.

Engage in Theft Detection Incentive Scheme

- The TDIS is not as effective as it is designed to be, with some parties not engaging or pro-actively completing theft detection activity. Instead, only acting on tip-offs.
- Targets for SME / B2B suppliers are believed to be overstated. Large suppliers, with mature theft detection processes, are failing to achieve them and do not believe them to be achievable.
- The overall process for submission of TDIS data via the REC Portal is cumbersome and time consuming particularly in relation to failed uploads.

Verbatim comments from the workshop can be found in Appendix 3

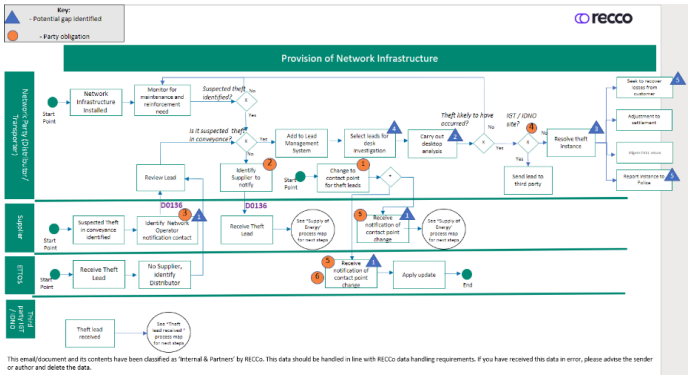
Output

A post workshop summary pack has been created capturing the revised versions of the process maps.

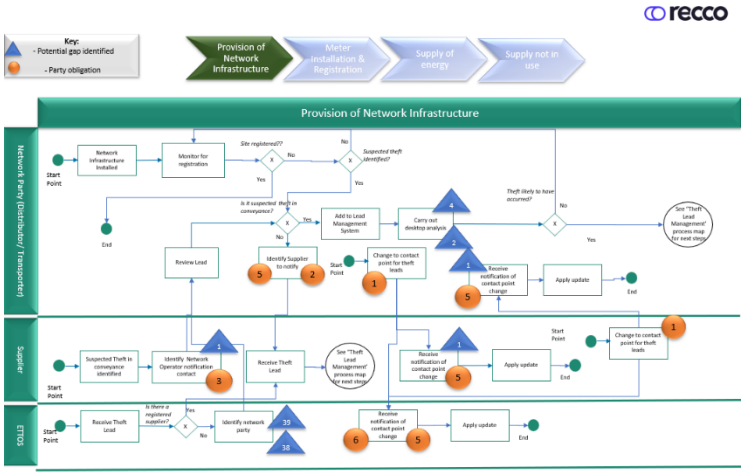
These can be accessed here.

An example of a revised process map has been included below for information. A more detailed summary of the gaps and recommended next steps is included in the "Gap Analysis Summary" section of this document.

Original process map (Provision of Network Infrastructure)



Revised process map (Provision of Network Infrastructure)



8 GAP ANALYSIS SUMMARY

Throughout this project, and as referenced earlier in the document, gaps identified were categorised into the following areas:

- Awareness / Incentive
- Monitoring / Reporting
- Obligation / Responsibility

A comprehensive log detailing all identified gaps has been created, which highlights similar themes. This section of the document dives into several gaps identified and where appropriate provides recommendations on potential actions and next steps.

Further gaps can be explored in Appendix 4.

Awareness / Incentive

8.1 TDIS participation

Prior to this project there has been a hypothesis that the TDIS is not as effective as it is intended to be. One party confirmed they have limited engagement with TDIS. This is due to the reward of achieving TDIS targets not outweighing the cost of conducting pro-active theft detection and prevention within their organisation. The party confirmed they investigate all external tip offs received, such as those from ETTOS or a member of the public, however, they conduct minimal pro-active theft detection outside of this and informed REC, via the workshops, that is more cost effective for them to pay into the TDIS scheme than establish a formal theft detection function internally.

In addition to this a B2B supplier confirmed they have mature theft detection process in place, however, typically they are not able to meet the targets set as part of the TDIS and are regularly

required to pay into the scheme. The narrative provided by the representative of this organisation indicated the targets are not accurate. In their experience the volume of theft incidents targeted is not representative of the level of Energy Theft they detect within their customer base on a regular basis. This is due to their experience of large consumers rarely committing Energy Theft. Their suggestion is the methodology used for creating the targets should factor this in.

They will, however, continue to engage with the scheme as it is a licence and code obligation.

Based on this anecdotal feedback it may be reasonable to conclude that other organisations are not engaging with the TDIS for the reasons outlined above. The TDIS would benefit from a review to ensure it is effective, promotes the desired behaviours and achieves what it is designed to.

A contributing factor to this is which outcomes the scheme rewards – currently it rewards successfully detected thefts only and does not factor in the cost and effort exerted to investigate all leads to identify those thefts and remove non thefts from a lead sample. In the scenario in which a party has a conversion rate of 25% of investigations conducted being confirmed thefts, currently under the TDIS they would be rewarded for the 25% not the other 75% however in real terms there may be little to no difference in the cost of investigating those leads.

The scheme also does not factor in the quality and accuracy of reporting into the TDIS. As with the previous point parties are rewarded for reporting a theft as confirmed however, if the supporting information (such as the estimate of unrecorded energy) is not accurate or reflective of the situation and is potentially not relevant it does not get reviewed / penalised. This could lead to un-intended behaviours such as parties completing TDIS reports with little to no information beyond that theft was identified.

In addition, several parties indicated the physical process of uploading TDIS data to the REC Portal can be cumbersome and time consuming, particularly relating to errors with TDIS submissions. Users are notified that an upload has failed, however, they are required to go through their submission file line by line to determine where the error occurred or raise a ticket with the Service Desk to gain further information.

Alongside this several fields do not have any form of value / volume-based validation, simply whether the field has a value. This often leads to inaccurate information being captured and can lead to under reporting of the scale of the problem, for example where the volume of kWh is not entered. The field needs to be populated in order to upload the file; however, the value is not validated. If this information is accurately captured it could increase the accuracy of the theft estimation and potentially improve settlements.

Recommendations

- Conduct a full end to end review of the TDIS to determine whether the scheme should be amended to better incentivise participation. Particular focus should be given to how smaller suppliers / those with limited resources can be better incentivised to engage with the scheme effectively. This should include how the scheme can be made more cost effective for smaller parties to ensure the cost and effort of detecting theft is factored into the rewards.

- Monitor current and historic participation in the TDIS to determine which parties are consistently failing to engage and consider if additional Performance Assurance activities are needed for scenarios in which parties do not fulfil their code and/or licence obligations relating to Energy Theft. Such Performance Assurance activities may include the quality and accuracy of the data submitted into the TDIS or the number of ETTOS leads that are investigated.
- Review the TDIS submission process to identify changes that would improve the overall user experience.

8.2 Evidence collection, retention and access

During the workshops, Energy Suppliers identified several challenges faced following a confirmed instance of Energy Theft, when attempting to document evidence for the purposes of calculating losses and potentially passing for prosecution. These included:

- Parties responding to emergency safety related cases are inconsistently capturing and providing accurate information on the scale of the illegal installation once it has been resolved. This includes the volume and detail of equipment that was using unrecorded energy. E.g., Number of water pumps or computer servers. Following a review by ETREG members it was highlighted that the primary role of the network engineer is to make the site safe by appropriate means and not act in an RP context. They do not have the requisite skills to act in this capacity.
- Difficulty in contacting the relevant teams within Network Parties to gain further information and detailed discussions relating to Energy Theft.
- Gaining supporting information from Police services can be difficult and time consuming.
- Access to removed meters to support a prosecution as they can often be stored with insufficient record keeping to be able to readily access them. Including an audit trail of how the evidence has been stored, managed and accessed that would meet PACE requirements for use in a future prosecution.

This combination of issues can act as a dis-incentive for suppliers to pursue Energy Theft to prosecution or accurately being able to report losses into settlement. It may also contribute to the low success rate of prosecutions for Energy Theft, as outlined in the analysis of Police data (included earlier in this report).

Recommendations

- Review and refresh the tools and resources made available to parties to calculate losses resulting from Energy Theft. Factor in new types of theft drivers such as crypto mining
- Publication of Best Practice guidance and reference material on the importance of obtaining accurate evidence documenting Energy Theft taking into consideration the role of a Network Party during emergency callouts



- Explore the use of centrally provided secure, auditable and reportable mechanisms for sharing evidence obtained with relevant parties e.g., Photos of a tampered installation. One such option to consider may be the Secure Data Exchange Portal (SDEP).
- Engage with the Police to determine if there is an underlying factor contributing to the inconsistent reporting and access to information.
- Conduct an RFI with Network Parties to identify how they manage unregistered sites and identify any differences in processes across the industry.

8.3 Monitoring and reporting gaps

Data sharing and utilisation of existing data

Data sharing has long been considered a hindrance to detecting and preventing Energy Theft. Through the workshops and the ETREG (Energy Theft Reduction Expert Group) meetings, parties have highlighted the challenges they face when detecting other thefts that may have been committed by the same consumer or identified at the same property.

Outside of the TDIS there is no central repository for documenting Energy Theft. Parties have highlighted that this is an obstacle when determining if an individual has committed Energy Theft previously or if a premise has had a history of Energy Theft. Understanding this history would be valuable when detecting serial offenders.

Implementing such a repository would enable parties with a legitimate interest (e.g., Energy Suppliers or Network Parties) to determine if Energy Theft has occurred at a premise under investigation or if an individual has previously been involved in Energy Theft.

A scenario in which this could help would be if a landlord has multiple properties and one is under investigation. This would enable an Energy Supplier to update the repository to alert other suppliers which may supply some of the premises.

Owing to the nature of the data required for such a repository (personal details of individuals) there are a number of privacy and data protection principles to consider alongside access management. Such a repository could be operated and maintained by the Code Manager. Taking this approach would enable the data to be stored and accessed securely with the Code Manager maintaining placing strict controls to ensure data is not accessed / obtained by parties that do not have a legitimate interest.

Another area relating to data sharing is peer to peer sharing. There are often scenarios in which one industry party, (e.g., an Energy Supplier) needs to share information securely with another Energy Supplier regarding a suspected Energy Theft. This may be in the case that theft has been detected on a newly acquired supply and there is a suspicion the theft has been ongoing for a period prior to the new supplier's registration. Current processes utilise emails and dataflows, however, there is a risk with relying on emails in that they can easily be lost, remain unread or be difficult to access. This is especially prevalent when an organisation changes personnel and may not communicate this externally. There is also no easy, central way of tracking communications and actions resulting from these.

Creation and utilisation of a central mechanism would enable organisations to clearly identify Energy Theft that would be beneficial in several ways:



- Provide quick, easy access to share information on theft between parties;
- Enable monitoring of how often information on theft is shared between parties;
- If data sharing on theft increases, (e.g., flagging to new Suppliers where a customer has been found to be engaging in theft previously) a specific theft process type would provide a clear means for Suppliers to get additional information if needed.
- Quick and easy sharing of evidence such as photos of the theft (e.g., After a Network Party has been asked to make the site safe by the police)

One potential option to consider would be the SDEP.

Furthermore, there is an opportunity to utilise existing TDIS data for analytical purposes; to identify if a specific premise has had Energy Theft recorded on more than one occasion and identify any individual that has been linked to Energy Theft on more than once occasion. This information could then be utilised for targeted monitoring and has the potential to provide insight that could be used to detect Energy Theft elsewhere and for the development of robust deterrents.

Recommendations

- Consult with industry participants to determine if a central repository (outside of the TDIS mechanism) for documenting Energy Theft is desirable and feasible. If so, explore what mechanism would be the most suitable, giving due consideration to the need for it to be secure, auditable and reportable. One such option may be the SDEP.
- Utilise the TDIS data to enhance the analytical and insight capability into Energy Theft including:
    - Identifying if there are multiple theft instances reported against the same site.
    - Identifying if individual Consumers are linked to multiple theft reports.

8.4 Monitoring of sites with new connections & those post Energy Theft resolution

During the workshops, several participants highlighted gaps and process issues at both the start of the energy lifecycle and the end of the lifecycle.

These focused on a lack of consistent reporting to monitor sites at these stages as set out below:

- Following a new service installation, monitoring of sites to ensure Consumers register with an Energy Supplier in a timely manner;
- Following a supply interruption (for debt or theft related reasons or otherwise), monitoring of sites to ensure the service is not re-instated illegally;
- Once a service has been removed (for theft related reasons or otherwise) monitoring to ensure the service is not re-instated illegally



- Lack of a consistent, documented process to request a service removal on grounds of theft and a follow up process to prevent a consumer simply requesting a new connection.

In each scenario parties indicated they understood their obligations, however, parties can have varied approaches to this, with some being more pro-active than others.

In addition, Network Parties highlighted the limited abilities they have to resolve the situation in the event a Consumer does not engage with an Energy Supplier, or a supplier does not promptly engage with a Consumer that has expressed an interest in registering with a specific supplier. Ultimately, if a Consumer does not engage with a supplier, Network Parties are aware of their ability to be able to disconnect a site, however, this may not occur until a lengthy period after the supply has been connected, therefore, leading to an extended period where consumption has not been recorded. Likewise, where a supplier has been contacted but has not engaged with a Consumer, they are only able to escalate with a supplier, as it is not desirable or appropriate to disconnect the supply.

Recommendations

Explore the introduction of formal reporting requirements (under the auspices of the Performance Assurance function; and

Consider how this could be monitored and enforced to ensure it would drive the desired behaviours rather than being seen as a burden that is likely to further dis-engage parties and lead to non-compliance.

Develop a consistent process for parties to request a service removal and prevent a new service being installed before a theft is remedied.

Review the licence and code requirements placed on Network Parties to determine what is an acceptable course of action to take to prevent future energy theft occurring at a site. For example, denying a new connection to a consumer at a site that has had a service removed due to energy theft where there is deemed to be a high risk of re-offending in the future and where the consumer has / has not remedied (example where the outstanding charges have not been paid) the theft.

8.5 Police prosecutions

During the workshops participants highlighted the inconsistencies in relation to pursuing prosecutions once a theft instance has been resolved.

There is no clear central view of how and when theft is reported to the police and what the subsequent outcomes of these are. The data received from police forces as part of a freedom of information request made in October and November 2022 indicate that reporting records are inconsistent. Some forces provided detailed information on the volume of prosecutions taken forward and the outcomes whilst others were only able to provide high level information or none at all.



This suggests there is an inconsistent approach to record keeping across forces. It is also not clear how much information is kept by Energy Suppliers and Network Parties in this area. The analysis completed as part of this project indicates there is a large discrepancy between the volume of Energy Theft identified and reported and the volume of prosecutions. Based on this it is reasonable to assume that the majority of thefts found remain unreported to the police.

There are three factors to consider as to why this might be:

1. Parties are not clear on when to escalate Energy Theft to the police; and
2. Parties do not have visibility of the volume of cases that are being sent for prosecution; and
3. Parties do not have visibility of the success of cases that make it to prosecution, therefore, are less incentivised to report it due to the low success rate of prosecutions versus the effort and resource required to pursue a prosecution.

Based on this it is reasonable to conclude that the threat of prosecution has limited effect in acting as a deterrent to potential perpetrators.

Recommendations

- RECCo should consider publishing guidance in conjunction with the police, Crown Prosecution Service (and in Scotland, the Crown Office and Procurator Fiscal Service) and other organisations (such as Crime Stoppers) on when prosecutions should be pursued.
- Consider the need to capture and publish regular reporting detailing the progress and outcomes of Energy Theft and whether publishing this publicly will act as an additional deterrent to potential perpetrators.
- Consider publishing guidance on the ability to pursue a private prosecution in the event a public prosecution was not progressed.

8.6 Reporting losses into settlement

Information provided by Elexon during the workshops indicated there are inconsistent approaches to accurately calculating and reporting electricity Energy Theft losses into settlement.

Elexon indicated some suppliers regularly report unrecorded consumption accurately for each confirmed theft, however, others do not. This was a view echoed by Xoserve in relation to gas consumption. The treatment of electricity Energy Theft losses identified after the 14 month (RF) settlement window were also highlighted. Currently there is no clear way of managing this and it is likely to be exacerbated when Market Wide Half Hourly Settlement goes live; the final settlement window will close after 4 months for those sites migrated to half hourly settlement post go-live. This will likely result in a significant increase in the volume of energy not entering settlement with the defined timescales.

Due to the nature of how losses are accounted for and recovered (unallocated losses are socialised across the industry) this can have the unintended consequence of parties who accurately report into settlement paying twice – for both the unrecorded energy calculated from their own Consumers and a share of the unallocated volume for the rest of the industry.

This has the potential to act as a disincentive for suppliers to accurately report, as per their obligation, knowing that others will not be doing this.

Following further discussions with Elexon it was established there is currently no specific theft related guidance available on the process that should be followed to enter unrecorded energy into settlement.

Recommendations

- Engage with Elexon and Xoserve to develop and publish Best Practice guidance material on how to enter unrecorded energy correctly into settlement.
- Engage with Elexon and Xoserve to determine if additional performance assurance monitoring is needed within the codes of practice (BSC, UNC, REC) to ensure all parties act consistently or if an alternative incentive could be implemented to encourage the desired behaviours.
    - For example, suppliers regularly and correctly entering energy into settlement could pay for a lower proportion of the unallocated energy charge.
- Continue discussions with Elexon and Xoserve to explore a process for recording and allocating unrecorded losses linked to Energy Theft after the final settlement window has closed.
- Conduct a review of both the electricity and gas settlements processes in relation to Energy Theft to understand the differences in each and where the processes may be streamlined / duplicated to ensure losses due to Energy Theft are entered correctly and paid for appropriately.

Obligation / Responsibility

8.7 Objection to a change of supplier request

A common problem that has been identified by suppliers is the ability for Consumers to change supplier during an Energy Theft investigation. The challenges that arise here are:

- Moving to a new supplier during an active investigation effectively means the investigating supplier can no longer proceed with a site visit to confirm Energy Theft, resulting in the investigation ceasing. With limited ability to share information with the new supplier this effectively means the new supplier must start from scratch prolonging the instance of theft
- Moving to a new supplier after Energy Theft has been resolved limits a supplier's ability to successfully recover the costs of unrecorded energy



- A new supplier is only able to back-bill for the period they have been the registered supplier meaning a consumer can avoid paying for large volumes of energy across multiple suppliers
- In many cases Consumers can gain a new service / re-instate the existing service with a new supplier as the new supplier is not likely to know the service has been removed / restricted due to Energy Theft

Currently there is no mechanism or process in place for a supplier to object to a change of supply request for reasons related to Energy Theft. This can result in a perpetrator continually switching supplier to avoid detection leading to the theft continuing for a longer period than necessary not only increasing the financial impact of the theft but also endangering the safety of individuals.

Since faster switching has been in place, suppliers have provided anecdotal evidence that this problem is increasing due to Consumers switching supplier before the investigating supplier is able to act and potentially before any suspicion.

Recommendations

- Conduct a thorough and detailed assessment of the level of Energy Theft that goes undetected or continues longer than necessary due to Consumers changing supplier
    - One such approach could be a consultation / request for information to suppliers to gain the required information
    - Overlaying switching data against TDIS data could also provide insight. DCC hold switching info at MPxN level so could be engaged to explore this. In addition, the TDIS data contains information (supplier outcome code L) which could also be utilised
- Explore with impacted participants, Ofgem and Consumer groups if such a change is feasible and if so, how it could be implemented effectively giving due consideration as to how the use of such an objection can be monitored to ensure it is not mis-used by suppliers.

9 RECOMMENDATIONS SUMMARY

9.1 Awareness / Incentive

- Conduct a full end to end review of the TDIS to determine whether the scheme should be amended to better incentivise participation. Particular focus should be given to how smaller suppliers / those with limited resources can be better incentivised to engage with the scheme effectively. This should include how the scheme can be made more cost effective for smaller parties to ensure the cost and effort of detecting theft is factored into the rewards.
- Monitor current and historic participation in the TDIS to determine which parties are consistently failing to engage and consider if additional Performance Assurance activities are needed for scenarios in which parties do not fulfil their code and/or licence obligations relating to Energy Theft. Such Performance Assurance activities may include the quality and accuracy of the data submitted into the TDIS
- Review the submission process to identify changes that would improve the overall user experience
- Review and refresh the tools and resources made available to parties to calculate losses resulting from Energy Theft. Factor in new types of theft drivers such as crypto mining
- Publication of Best Practice guidance and reference material on the importance of obtaining accurate evidence documenting Energy Theft
- Explore the use of centrally provided secure, auditable and reportable mechanisms for sharing evidence obtained with relevant parties e.g., Photos of a tampered installation. One such option to consider maybe the SDEP
- Engage with the Police to determine if there is an underlying factor contributing to the inconsistent reporting and access to information
- Conduct an RFI with Network Parties to identify how they manage unregistered sites and identify any differences in processes across the industry

9.2 Monitoring / reporting

- Consult with industry participants to determine if a central repository (outside of the TDIS mechanism) for documenting Energy Theft is desirable and feasible. If so, explore what mechanism would be the most suitable, giving due consideration to the need for it to be secure, auditable and reportable. One such option may be the SDEP.
- Utilise the TDIS data to enhance the analytical and insight capability into Energy Theft including:
    - Identifying if there are multiple theft instances reported against the same site.
    - Identifying if individual Consumers are linked to multiple theft reports.



- Explore the introduction of formal reporting requirements (under the auspices of the Performance Assurance function) for REC parties to report on the status of MPxNs that are not registered with a supplier and/or are not energised; and
- Consider how reporting requirements on the status of unregistered and or de-energised MPxNs could be monitored and enforced to ensure it would drive the desired behaviours rather than being seen as a burden that is likely to further dis-engage parties and lead to non-compliance.
- Develop a consistent process for parties to request a service removal and prevent a new service being installed before a theft is remedied.
- Review the licence and code requirements placed on Network Parties to determine what is an acceptable course of action to take to prevent future energy theft occurring at a site that has previously had a service removed due to theft activity. For example, denying a new connection to a consumer at a site that has had a service removed due to energy theft where there is deemed to be a high risk of re-offending in the future and where the consumer has / has not remedied (E.g., where the outstanding charges have not been paid) the theft.
- RECCo should consider publishing guidance in conjunction with the police, CPS and COPFS and other organisations (such as Crime Stoppers) on when prosecutions should be pursued.
- Consider the need to capture and publish regular reporting detailing the progress and outcomes of Energy Theft and whether publishing this publicly will act as an additional deterrent to potential perpetrators.
- Consider publishing guidance on the ability to pursue a private prosecution in the event a public prosecution was not progressed.
- Engage with Elexon and Xoserve to develop and publish Best Practice guidance material on how to enter unrecorded energy correctly into settlement.
- Engage with Elexon and Xoserve to determine if additional performance assurance monitoring is needed within the codes of practice (BSC, UNC, REC) to ensure all parties act consistently or if an alternative incentive could be implemented to encourage the desired behaviours.
    - For example, suppliers regularly and correctly entering energy into settlement could pay for a lower proportion of the unallocated energy charge.
- Continue discussions with Elexon and Xoserve to explore a process for recording and allocating unrecorded losses linked to Energy Theft after the final settlement window has closed.

9.3 Obligation / Responsibility

- Conduct a thorough and detailed assessment of the level of Energy Theft that goes undetected or continues longer than necessary due to Consumers changing supplier



    - One such approach could be a consultation / request for information to suppliers to gain the required information
    - Overlaying switching data against TDIS data could also provide insight. DCC hold switching info at MPxN level so could be engaged to explore this. In addition, the TDIS data contains information (supplier outcome code L) which could also be utilised
- Explore with impacted participants, Ofgem and Consumer groups if introducing a change of supplier objection on theft grounds would be feasible. If so, explore how such a change could be implemented effectively giving due consideration as to how the use of such an objection can be monitored to ensure it is not mis-used by suppliers.

10 NEXT STEPS

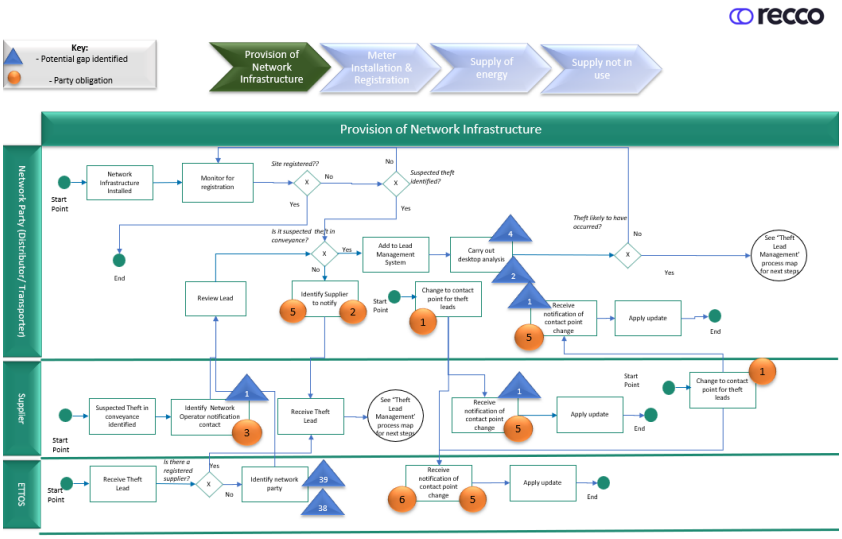
Following the publication of this report, RECCo will review and to the extent they do not already form part of the Energy Theft Reduction Programme, prioritise each of the recommendations identified within this document to determine which are to be taken forward. This should take into, consideration the complexity, costs and potential impacts/benefits of each recommendation and any inflight and planned activity.

11 APPENDIX

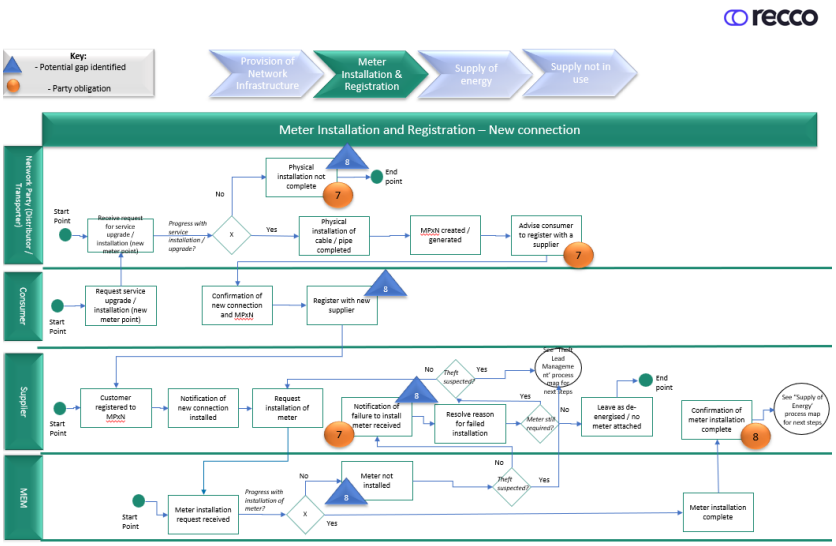
11.1 Appendix 1: Process maps

Document containing all process maps - Link

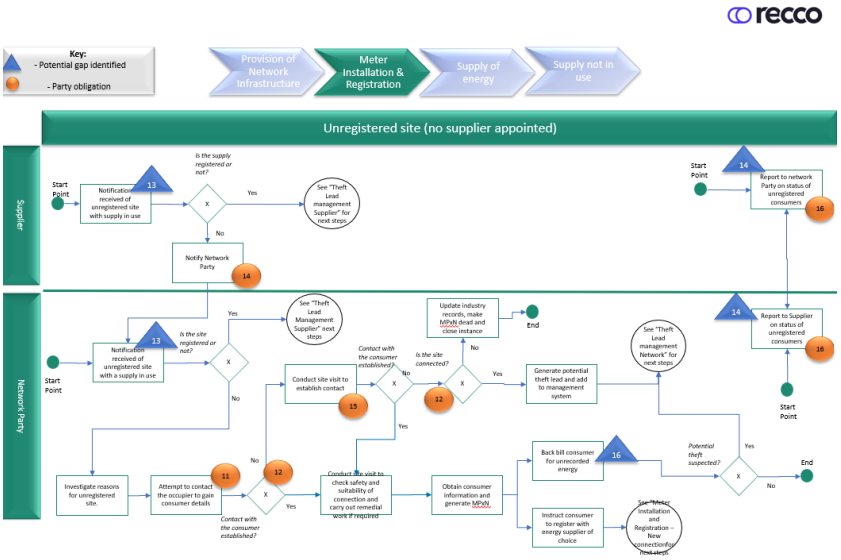
Provision of Network Infrastructure



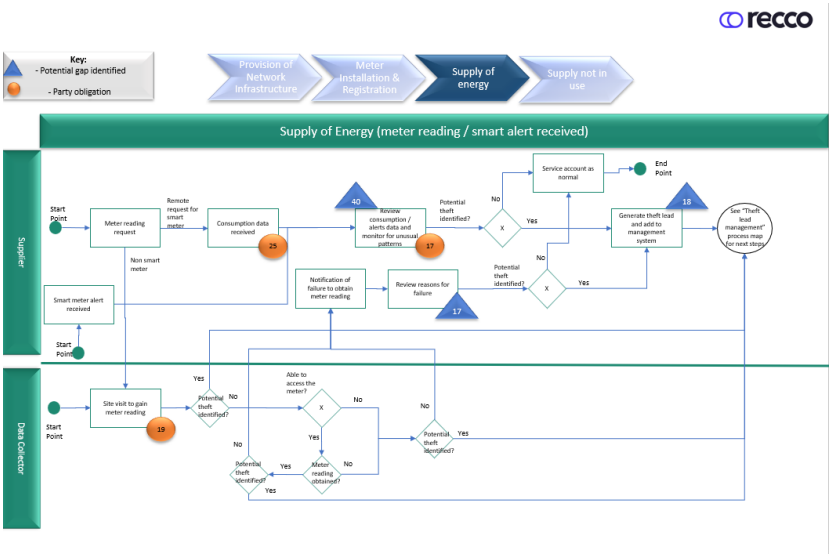
Meter installation and Registration – New Connection



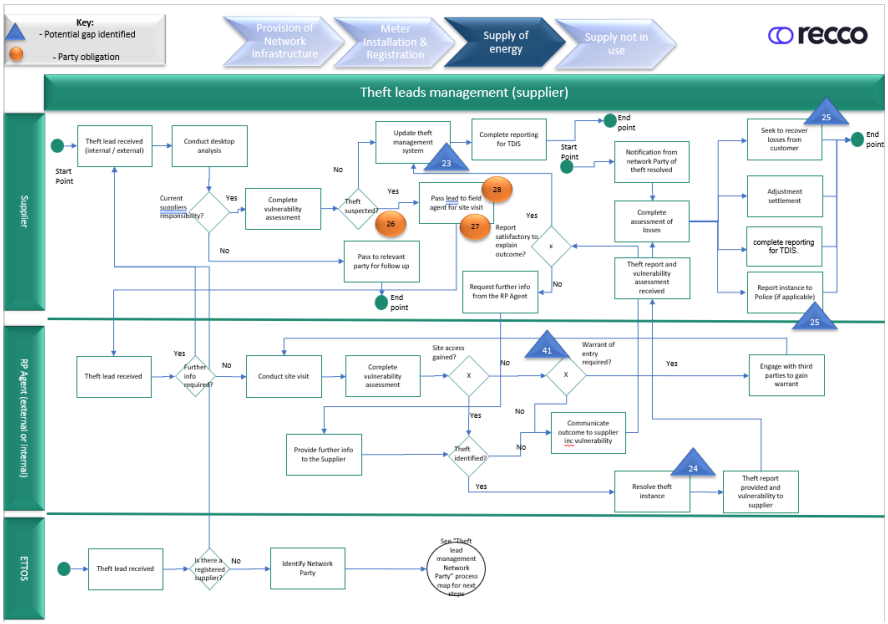
Unregistered site (no supplier appointed)



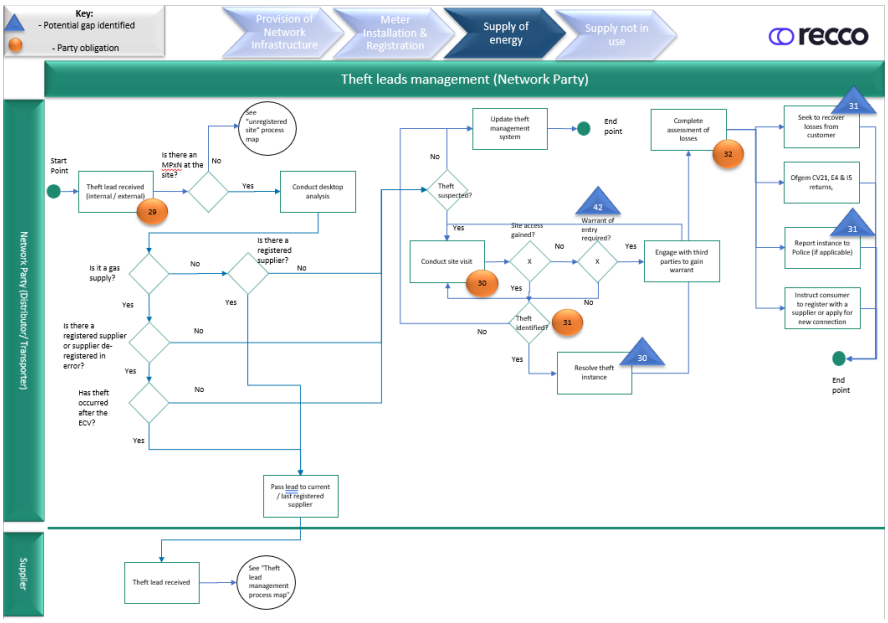
Supply of Energy (meter reading / smart alert received)



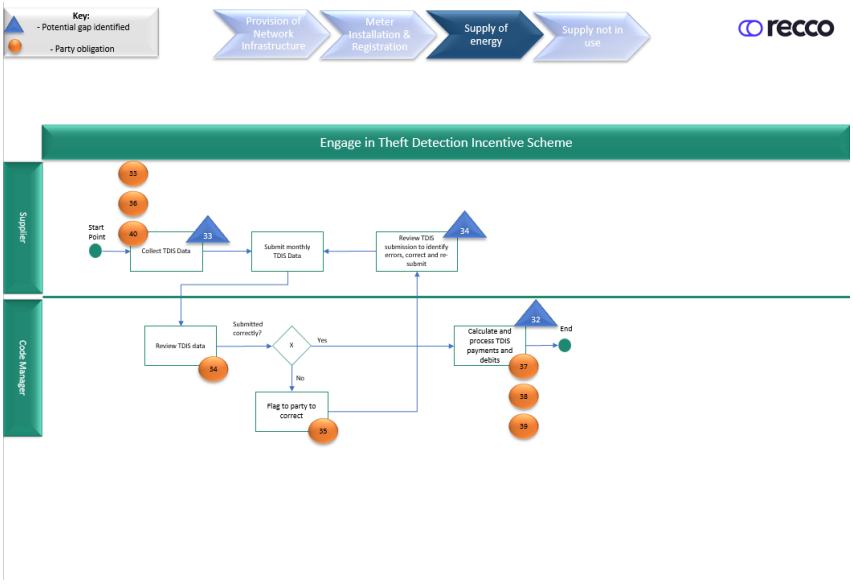
Theft leads management (supplier)



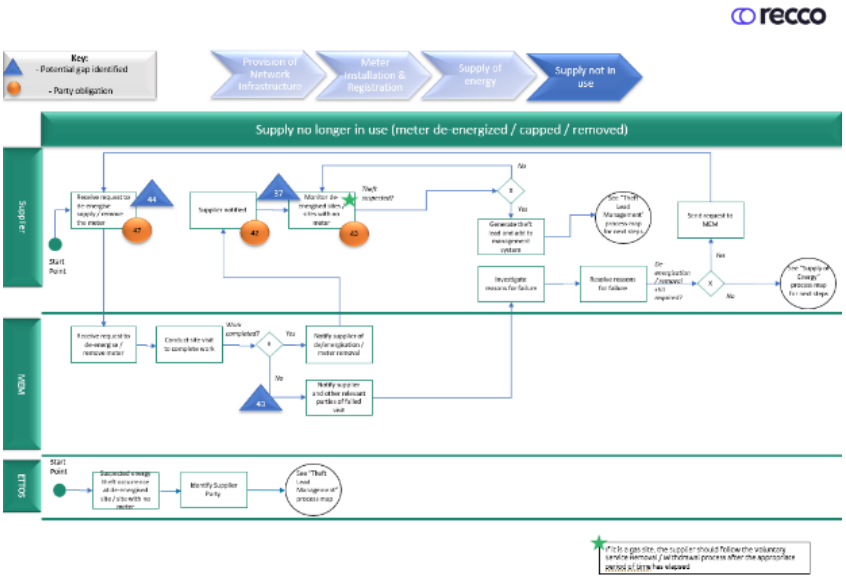
Theft leads management (Network Party)



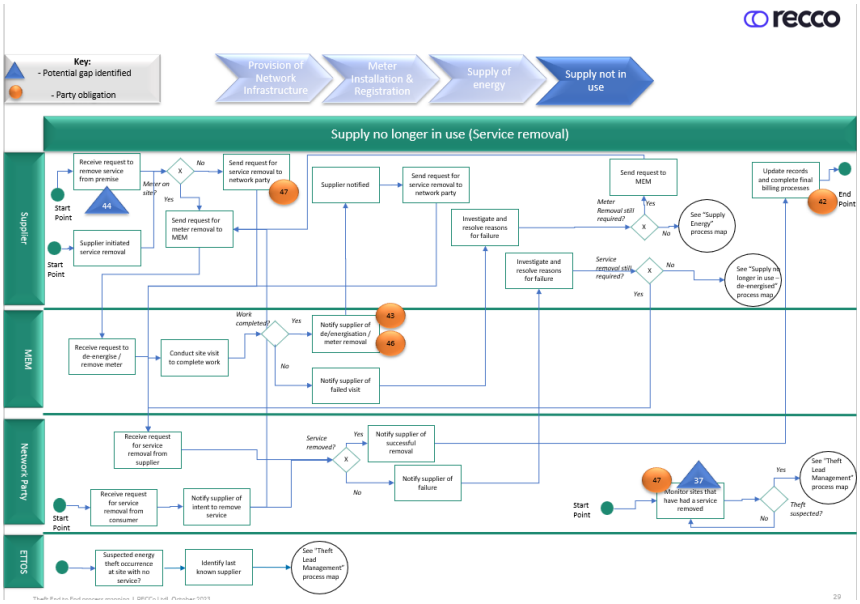
Engage in Theft Detection Incentive Scheme



Supply no longer in use (meter de-energised / capped / removed)



Supply no longer in use (service removal)



11.2 Appendix 2: Reference log documents

REC – Unbilled energy code of practice (schedule 8)

https://digital-navigator.azurewebsites.net/codes-schedules/24/3.2.0#sec1665

Ofgem DCP372 – Changes to the Theft Code of Practice

https://www.ofgem.gov.uk/publications/dcp372-changes-theft-code-practice

REC – Energy Theft Reduction (schedule 7)

https://digital-navigator.azurewebsites.net/

Ofgem Gas Supply standard licence conditions

https://www.ofgem.gov.uk/sites/default/files/2023-03/Gas%20Supply%20Standard%20Consolidated%20Licence%20Conditions%20-%20Current.pdf

Ofgem Electricity Distribution Consolidated Standard Licence Conditions
https://www.ofgem.gov.uk/sites/default/files/2023-03/Electricity%20Distribution%20Consolidated%20Standard%20Licence%20Conditions%20-%20Current.pdf

Ofgem Electricity Supply Standard Consolidated Licence Conditions
https://www.ofgem.gov.uk/sites/default/files/2023-03/Electricity%20Supply%20Standard%20Consolidated%20Licence%20Conditions%20-%20Current.pdf

11.3 Appendix 3: Selected workshop verbatim comments

Theft Lead Management (supplier)

- Suppliers are to take on shipper-less or unregistered sites where a meter is found, and gas is being consumed.
- There are data quality issues within the central systems, notably with theft being reported against an invalid MPRN.
- Prepay meters should be fully registered as customers are paying but they are not linked to an MPRN.

Theft Lead Management (Network Party)

- Suspected theft in conveyance cannot happen if there is a registered supplier for electricity supplies. For gas any theft identified before the ECV is theft in conveyance.
- Suppliers must install meters prior to an MPRN being linked.
- There is a delay in Xoserve being updated with incoming supplier information and where there are Xoserve rejections, these are not being followed up.
- DNs encounter issues with Xoserve address records as they are not maintained appropriately. The customers may be billed against an MPRN with incorrect details.

Provision of Network Infrastructure

- The ETTOS service primarily identifies the supplier. If this is not possible, DNO/Xoserve is approached. The information is passed to the supplier when identified, or the DNO deals with it if the supplier cannot be found. Safety concerns are flagged to the relevant emergency number by phone, then passed on to the supplier. Once the relevant party has the information, they carry out the analysis and pass it on to the RP team.
- If suppliers identify a supply point without an MPRN, they should follow the MNC process via the Xoserve or report to the DN to investigate.
- The last stage of resolving theft should be to register the premises with a supplier.

Unregistered sites and Consumers

- Sites can be unregistered however Consumers can only be unknown. Suppliers would then contact the Consumer to find out more information.



- Suppliers may be wary of disconnecting a Consumer as they may incur reputational damage, or the affected party may be a vulnerable customer.
- Network Parties have historically had issues identifying a MAM or tracing who originally installed a meter due to a lack of access to data. Customers are asked to contact the supplier of their choice to organise a contract however customers struggle to organise a contract for shipper-less MPRNs as some suppliers are not aware of the process or refuse to take shipper-less MPRNs.

Engage in Theft Detection Incentive Scheme

- Errors in reporting through the TDIS scheme need to be clearly communicated to parties in detail, to enable easy understanding of how to resolve the errors. The current format is not user friendly, so the process becomes time consuming.

11.4 Appendix 4: Gap and reference log

Link to the Gap and Reference log