RECCo ENERGY THEFT PORTAL SPECIFICATION OF REQUIREMENTS

1 Context

This proposal focuses on the development of a centralised repository for data from across the Industry relating to investigations into reports of suspected or actual energy theft to support the wider REC Theft Reduction Strategy.

This centralisation of 'Criminal Offence' data will provide increased visibility of the scale of the problem, the efforts of Industry Party's to address it and the overall effectiveness of the REC Theft Reduction Strategy.

2 Requirements & Scope

This document focuses on our view of an appropriate solution.

Minimum Specification

We believe the following functionality is likely to be the minimum specification of any service offered albeit delivered in phases: -

- Secure access for all REC Parties[1] and their representatives
- Data submission facilities to include individual record input and bulk upload by file transfer
- Bespoke dashboards/reporting suite
- Heatmapping
- Trend analysis
- Repeat offending alerts
- Health & Safety Incident log and reporting facility
- Interface capability to support an independent prosecution unit
- Evidence Log repository
- Input of public domain data to support trend analysis and lead generation

Secure access for all REC Parties and their representatives

REC Parties and their agents involved in Revenue Protection activity will require secure access to the system and any reports generated pertinent to their activity for a number of their representatives with a variety of functions and capabilities. It is likely there will be in excess of 100 different organisations, each with multiple roles accessing the service and potentially some variation in the visibility of their Party's data dependent upon role or profile. In addition there will be some requirement for a socialised view of data submitted by other parties.

Data management and security mechanisms will need to be in place, sufficiently robust to allow the level and detail of reporting to individual parties as required but without breaching confidentiality and data protection principles, particularly where Revenue Protection Service Providers (RPS) work on behalf of a number of energy suppliers.

Data submission by individual record input or bulk upload by file transfer

The solution will need to offer parties the flexibility to upload and update individual records directly or submit files for bulk upload by secure file transfer or similar. If data can be submitted in a variety of

[1] The following categories of person are eligible to become a Party under the Retail Energy Code – DCC; RECCo; Energy Suppliers; Gas Transporters; Distribution Network Operators; Metering Equipment Managers

formats, appropriate validation will need to be in place to ensure consistency. There may be a requirement for parties to have access to both options for different role profiles.

Bespoke dashboards/reporting suite

A series of dashboards, graphs or similar reporting is needed to allow Energy Suppliers a comparative view of their performance against KPIs in specific areas, how their overall performance compares to the rest of the Supplier Community and the propensity for specific tampers in localised areas and nationally. It will also include monthly reports showing current and cumulative performance against individual and overall Theft Detection Incentive Scheme targets. If Parties are able to view their data in the format of their choice it will enhance their user experience.

The REC Code Manager[2] may require additional dashboards to enhance or supplement their performance assurance regimes and it is possible there will need to be the option of bespoke or ad-hoc reporting either for individual parties or for advanced performance assurance monitoring whereby trends indicate an issue with a Revenue Protection Service Provider performance across multiple parties.

Heatmapping

The development of industry level heat maps to show where theft investigations have taken place and the various possible outcomes:-

- Each individual supplier will have a view with their own submissions highlighted and the rest of the Industry's performance will be displayed but anonymised at both supplier and specific property identifier level.
- For their own entries, a Supplier will be able to drill down into specific details of each of the cases.
- This industry wide view will provide visibility of areas with minimal/no reports of suspected theft and will help drive the decision making behind where ETTOS/SES local media and/or Out of Home campaigns should be run or drive increased supplier proactivity in these areas.
- The REC Code Manager will have visibility of each individual Suppliers submissions for the purposes of managing the Energy Theft Detection Incentive Schemes.

Heatmaps and dashboards will need to be updated regularly as new data is uploaded to the central repository. A decision will need to be made to determine whether this is done each time any additional data is added or if it's a weekly/monthly refresh.

Trend Analysis

Trend analytics to be developed to highlight anything that may assist the industry in the identification of energy theft, e.g.

- the prevalence of particular tampers in an area
- a new tamper identified and increasing numbers being reported
- possible links to organised crime, whether it's the same perpetrators on multiple jobs or individuals selling a service to tamper with meters
- consistent differences in the conversion rates by specific suppliers or Revenue Protection Service Providers.

Repeat Offending Alerts

[2] The REC Code Manager is a person/persons appointed by the REC Board to perform those tasks and functions expressly ascribed to it under the REC to assist in the smooth and effective operation of the REC

An alert mechanism to notify incoming Energy Suppliers of properties with multiple reports of confirmed energy theft over a specified period, triggered at change of supplier with no recent change of customer and compliant with the appropriate data protection legislation. This will allow suppliers to implement closer monitoring in these situations.

Health & Safety Incident log and reporting facility

Alongside the dangers associated with energy theft itself, the agents and operatives working in this field are often subject to verbal and physical abuse, threats of violence and assaults. This solution should provide a reporting mechanism for these details to be recorded by the party involved sufficient to support criminal investigations if appropriate but also to create a comprehensive record of incidents to be accessible by all parties involved in the detection and prevention of energy theft to try ensure the safety of all frontline agents.

Interface capability to support an independent prosecution unit

RECCo is investigating the development of a partnership operation similar to the Insurance Fraud Investigations team to take responsibility for determining the energy theft cases that reach the public interest threshold for a criminal prosecution. Any police task force would require access to the system to analyse the data necessary to take cases forward and update the records so Energy Suppliers can track the progress of any Police investigations.

Energy theft can have links to organised crime groups such as modern-day slavery, people trafficking or someone other than the end user committing the act etc. but individual suppliers dealing with cases in isolation may not identify a pattern in specific areas whereas whole community data may provide the visibility to pursue criminal prosecutions.

Evidence Log repository

Energy Suppliers have an Obligation under the Electricity Act to notify the Police of all cases of tampering where the metering equipment has been exchanged or removed and hold on to the tampered equipment for a minimum of 6 months after the date of notification to the Police unless asked to retain it for longer to support a Prosecution.

Each Energy Supplier is currently responsible for notifying each Police force area of their activity, generally at the end of each month. Not all suppliers do and not all Police Force areas take any action as a result of the notifications they do receive.
This solution will generate a cross Industry report for each Police Force area ensuring all Suppliers are complying with their obligation in this area.

Input of public domain data to support trend analysis and lead generation

Supplementing the information provided by our Industry with the data provided by other Crime prevention groups may assist in identifying links to organised crime groups

Overlaying public domain data such as indices of Multiple Deprivation, Crime data or business types may assist the identification of trends by customer type/demographic and this could result in potential lead generation.

3 Timings and Project Delivery

We believe a phased approach to the development and delivery of the service is most appropriate. This will allow REC Parties the opportunity to input into the design of each subsequent phase, ensuring

the enhancements remain relevant and deliver functionality to support progression of the Energy Theft Reduction Strategy.

In addition, processing improvements and any advancements in technology can be applied with each phase update.

If it is not available in the initial phase delivery, development will be required to allow real time creation and update of records by direct input in addition to any batch or file upload facility. This will allow details of leads or tip-offs to be entered on receipt to create the record and then allow any subsequent updates to be uploaded at all stages of the investigation, including by the RPS agents working in the field.

This would facilitate proactive lead generation by field agents regardless of Supplier and reallocation of open investigations where a change of supplier occurs before an investigation is completed.

The suggested phases of development and deliverables are detailed below: -

Phase 1 – Theft trends, bespoke dashboards and heat mapping generated from current Theft Detection Incentive Scheme (TDIS) submissions

Energy Suppliers currently submit details of confirmed energy thefts for inclusion in Fuel specific 'Theft Detection Incentive Schemes' via the REC Portal[3] but the data items required to be submitted for each entry into the scheme is minimal in comparison to the total data items held for each suspected energy theft investigation.

A number of Energy Suppliers submit similar data items for all completed suspected energy theft investigations, regardless of the outcome of the investigation and this detail will allow complete visibility of theft investigation and detection activity across the industry.

Phase 2 - Additional data requirements to support centralised Prosecutions Unit for organised crime etc.

If agreement can be reached with a suitable partner to develop a process for progressing cases of energy theft for prosecution where it is deemed to be in the public interest, there will be a requirement for much more granular detail to be extracted from the investigation records to build the required evidence packs.

Any prosecution unit is likely to require details of cases that meet specified criteria or have commonality of perpetrator and the extraction of all relevant cases for review will need to be automated.

In addition, a central evidence repository is required to facilitate consistent reporting of all cases of abstraction completed each month by all REC Parties to satisfy the requirement for disposal of tampered electricity meter evidence in cases where there is no benefit or public interest case to support prosecution.

Phase 3 - Additional dashboards developed as required by Industry when agreement is secured for additional data provisions

Additional dashboards or data requirements are not specified at this time as these will be determined by REC Party requirements and any requests for REC Parties to provide additional data items in specified formats will need to be approved via the REC Change Process.

This phase of the proposed solution will need to accommodate all data items that may be collated as part of energy theft investigations, regardless of the outcome, to provide a greater opportunity for

[3] The REC Portal is the online platform which acts as a repository to all information relevant to the Retail Energy Code. Launched on 01 September 2021, it is designed to facilitate the dissemination of code information and promote effective two-way communication between the Code Manager and code users.

in-depth analysis, e.g.- identification of areas with higher than average cases of energy theft or specific tamper types; where there appear to be links to organised crime or the same name is provided for the perpetrator of the tampering, etc.

Data items must be stored to allow maximum filtering opportunities.

It is possible there may be a requirement for enhanced Performance Assurance reporting, e.g. a comparison of conversion rates by lead types, tip off sources, tamper types etc. and how individual REC parties and their agents perform in comparison to the industry performance for each of the areas reviewed.

Phase 4 - Alerts, lead generation following introduction of data from other public bodies e.g. indices of deprivation etc.

Some REC Parties have previously requested a system to provide visibility of health and safety alerts relating to threats of violence and physical or verbal abuse against Revenue Protection and other industry field agents. The ability to capture this level of detail on investigations for it then to be made available to all REC Parties will be the starting point.

Not all threats come from the consumer being investigated, often from neighbours or others in the vicinity so any alerts would be to create awareness of areas where extra vigilance is required.

This phase may also include the import of public domain data, including but not limited to 'indices of deprivation', to assist with trend analysis and for use in any potential future lead generation.

Phase 5 - Exploration of data
The wealth of data held in the solution by this point may have other uses that have not yet been considered.

Learnings from consumption patterns and tampering cases could give rise to earlier interventions, particularly in hardship cases, but there will likely be many possibilities and opportunities.

We hope to be in a position to start development of the solution during the 2023/24 Theft Detection Incentive Scheme year so this data can be used to populate the solution for testing purposes before uploading historical scheme year data.