UTILITY THEFT AND EFFORTS AT PREVENTION: THE UNITED ENERGY DISTRIBUTION COMPANY’S EXPERIENCE

GEORGIA ENERGY SECURITY INITIATIVE

CONTRACT NUMBER 114-C-00-03-00063-00

JULY 6, 2006
UTILITY THEFT AND EFFORTS AT PREVENTION: THE UNITED ENERGY DISTRIBUTION COMPANY’S EXPERIENCE

GEORGIA ENERGY SECURITY INITIATIVE
CONTRACT NUMBER 114-C-00-03-00063-00

JULY 6, 2006
Utility Theft and Efforts at Prevention: The United Energy Distribution Company’s Experience

Georgia Energy Security Initiative
Contract Number 114-C-00-03-00063-00

© PA Knowledge Limited 2006
This report describes the major methods that have been used by customers and employees for electricity theft against the United Electricity Distribution Company (UEDC) in Georgia and the UEDC’s successful response against these attacks.

Commercial customers, often supplied by three-phase service connection, have the greatest motivation and means to steal electricity. They consume very large amounts of electricity, have the most to gain by accessing electricity illegally, and have the means to devise and implement sophisticated methods of theft. As a result, electricity theft by commercial customers can inflict significant financial losses on the utility company.

The UEDC launched a large-scale and intensive program to expose and prevent unauthorized access to electricity. This effort included not only the deployment of staff to investigate suspect units but also the creation of separate departments, divisions, and special services, establishment of standard procedures, and a review of human resources policies. While the anti-theft activities are directed primarily toward the company’s own customers, the actions of other corporate actors in the energy market as well as the company’s own employees were the focus of concerted efforts to reveal and eliminate corruptive behavior.

In this report we review commonly used methods of theft, note how difficulties of detection vary across the methods, and share examples from our own investigations. We describe the strategies used by the UEDC to expose and prevent theft and stress that no one method or approach is sufficient. Rather, any anti-theft effort must develop a repertoire of tools and techniques as well as the perseverance and analytical mindset to apply and adapt them appropriately. A successful fight against electricity theft requires dedication to the program’s goals at all levels of the organization and a near tireless effort by investigators.

We conclude this report with a discussion of the main “lessons learned.” We caution readers, and recognize ourselves, that an anti-theft program cannot be static. While the program goals must be constant, the methods and field strategies must continue to evolve in order to stay abreast of ever-developing innovations devised by individuals and enterprises intent on gaining unauthorized use of electricity.
# TABLE OF CONTENTS

## Foreward

1. **Theft of Electricity**
   - 1.1 Secondary Current Circuit 1
   - 1.2 Secondary Voltage Circuit 11
   - 1.3 Slowing the Meter 20
   - 1.4 Tampering with Seals 29
   - 1.5 Bypassing the Meter 34
   - 1.6 Falsification of Meter Readings 38
   - 1.7 Meter “Doctor” 38

2. **Theft of Inventory**
   - 2.1 Contractual Fraud 40
   - 2.2 Diversion of Material 40
   - 2.3 Diversion of Vehicles 41
   - 2.4 Theft of Diesel and Petrol Fuels 41
   - 2.5 Leasing of UEDC Assets 41
   - 2.6 Falsified Receipts 41

3. **Organizational Structure of an Anti-Theft Program**
   - 3.1 Commercial Safety Department 43
   - 3.2 Organizational Policies and Procedures 45
   - 3.3 Internal Audit Authority 46
   - 3.4 Professional and Ethical Employees 46

4. **Strategy and Methods for Identifying Theft**
   - 4.1 Investigate and Study 48
   - 4.2 Surprise Night and Weekend Inspections 49
   - 4.3 Thematic Inspections 50
   - 4.4 The Government Standards Lab 50
   - 4.5 Hardening of Electrical Network and Metering Installation 50
   - 4.6 Hardened 10 kV Metering Outfit 51
   - 4.7 Inspection of Neighboring Power Sector Companies 56
   - 4.8 Eliminating Illegal Lines 57
   - 4.9 Detailed Inspections 57
   - 4.10 Checking Small Licensees 58
   - 4.11 Use of Photographs 58
   - 4.12 Improved Legal and Regulatory Framework 59
   - 4.13 Meter Seals 60

5. **Lessons Learned**
   - 5.1 Organizational Structure and Strategy 62
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2</td>
<td>Policies and Procedures</td>
<td>63</td>
</tr>
<tr>
<td>5.3</td>
<td>Human Resources and Staffing</td>
<td>63</td>
</tr>
<tr>
<td>5.4</td>
<td>Methods of Detection</td>
<td>63</td>
</tr>
<tr>
<td>5.5</td>
<td>Technical Designs and Field Practices</td>
<td>64</td>
</tr>
</tbody>
</table>
1. THEFT OF ELECTRICITY

1.1 Secondary Current Circuit

Interfering with the secondary current circuit provides three ways to steal electricity. These include tampering with the current circuit wiring itself, falsifying the current transformer ratio, and introducing a load transformer into the system. The first and third approaches under-report actual electricity consumption by affecting the meter. In the second method, electricity usage is calculated incorrectly during the billing process because the actual transformer ratio differs from that on record. We discuss and provide illustrations of each method.

1.1.1 Tamper with the Current Circuit Wiring

There are several ways to steal electricity by tampering with the current circuit wiring. Commonly used methods include a) shunting the secondary current wires with bridges, or jumpers, on the connector block; b) untying the secondary current wires; and, c) connecting a current circuit breaker somewhere along the secondary current wires. With each of these methods the customer’s “true” electricity consumption is under-recorded, because only partial (or no) electricity is supplied to the meter. Diagram 1 illustrates where illegal jumpers can be installed on current circuit wiring to steal electricity, and Photos 1, 2, and 3 document examples of such tampering.

The ease of detecting this general approach to electricity theft varies. If “bridges” are located near the meter, the theft is visually apparent upon inspection. However, a current breaker can be concealed outside the substation or the transformer building (also called a “kiosk” or transformer point), and it becomes relatively easy to avoid detection. For example, if an inspector enters a substation or transformer point, the employee who is on duty or another person involved in the theft can switch the breaker and the meter will resume working properly before the violation is revealed. After the inspector departs, the breaker switch can be changed again and the meter will stop recording electricity consumption. In one instance, UEDC staff discovered a breaker that was located in a desk drawer of the head of the enterprise. When the company representative visited the office, the head of the enterprise opened the drawer in a seemingly innocent fashion (e.g., to retrieve work materials or keys to facilitate the inspection) but also switched the breaker at the same time, thereby concealing theft of electricity.

Evidence of theft also was revealed in 220 kV and lesser substations when personnel who were on duty assisted the perpetrators by tampering with the current circuit wiring at metering points between the transmission licensee and the UEDC. (Similar methods are used to steal electricity by stopping or decelerating meters, and these are discussed in a subsequent section of this report.)
1. Theft of Electricity

Diagram 1 Tampering with the secondary current circuit

Photo 1 Shunting the secondary current at a connector block
1. Theft of Electricity

Photo 1 shows the current wires shunted (the extra blue, red and the black wires) on the connector block. This type of theft occurs most often during periods of large consumption when the “payback” for stopping the meter is greatest. This is a four-wire star (wye) connection and three currents must be shunted to stop the meter.

![Photo 1 Current wires shunted on connector block](image1.jpg)

Photo 2 Current wire released from the connector block

Photo 2 shows a current wire that is released from a connector block. Wire A630 is hanging free; it should be connected to the terminal to the right of wire B630 on the connector block.

Violations such as those shown in Photo 1 and Photo 2 are most frequently seen in high voltage metering points. The party stealing electricity cuts a voltage wire or shunts a current wire on, or before, a connector block. Because secondary commutation (that is, instrument transformer) circuits are typically quite old, it can be very difficult to determine if the wire was torn accidentally or if someone intentionally cut it, as is the case in Photo 2. If the current wires are shunted on a connector block (as shown in Photo 1), it is almost certainly intentional theft of electricity. However, we rarely encounter the latter method—it is outdated and only used at units operating in the nighttime, because it can be easily observed and there is a widespread perception that utility company inspectors do not conduct investigations at night or on the weekends.
1. Theft of Electricity

Photo 3 shows that the current wires between the current transformer and the meter are cut and then reconnected through a triple breaker. The triple breaker is in another room and the meter can be connected or disconnected from that location to hide the theft. This photo depicts the theft of electricity at a bread factory. Bags filled with wheat flour were placed on the breaker and we detected the device only after moving the bags of flour.

Electricity theft of the type illustrated by Photo 3 sometimes requires collusion with a contractor during the installation of a new metering circuit. For example, we have identified cases where the current and voltage cables of secondary commutation circuits are in a tube located somewhere between the current transformer and the meter. The tube provides ideal cover for a second, illegal line. The voltage wires are cut inside the tube and a separate line is laid from there to the interior of the factory or enterprise where it (the illegal line) is connected to the breaker, thus not registering the theft of electricity (for example, Photo 3 and Photo 14). The tube itself might be buried underground or under asphalt covering, further impeding detection.

1.1.2 Falsify the Current Transformer Ratio

Modifying or falsifying the transformer ratio is a widespread method of fraud. The customer installs a transformer with a higher turns ratio than what is on record in the billing office. As a result, the customer is billed for less electricity than is actually consumed.
1. Theft of Electricity

Briefly, each turn of the electric meter is multiplied by a number, or coefficient, associated with the transformer to compute electricity consumption and, hence, the electric bill. If the current transformer’s ratio is 200/5, then the coefficient K is 40 (200/5 = 40) and the meter reading is multiplied by 40 to compute consumption; if the ratio is 100/5 (K=20) then the meter reading is multiplied by 20, etc. The current transformer ratios and corresponding coefficients are recorded in the electric company’s billing system. Fraud can be executed by swapping out a current transformer for one with a larger (and unrecorded) turns ratio. For example, if a transformer with coefficient K=10 is removed and a current transformer with a higher turns ratio is installed in its place (e.g., K=20), then the customer will be billed for only 50 percent of the electricity actually consumed. Each turn of the meter will continue to be multiplied by 10 (the coefficient in the billing records) rather than 20.

This approach is far from new but it is relatively easy to hide and therefore attractive to perpetrators. A false manufacturer’s nameplate can be fastened onto the new transformer (i.e., one which has a higher turns ratio), but the label continues to report the (false) lower turns ratio that is registered in the billing system. Falsification is not detected without a detailed inspection of the transformer or by actually testing the unit. For example, field crews can use a device that creates a high current that is connected to the primary side of the transformer and then measure the actual current on the high side (e.g., the “100” side) and the low side (the “5” side). If the nameplate (and billing system) shows a ratio of 100/5 (K=20) and the field test readings are, say, 155 amps and 3.875 amps (or, K=40), the nameplate has been falsified and the customer is not being billed for all the electricity consumed. Even so, it can be difficult to prove intentional theft: A customer simply may claim that he or she purchased the current transformer without knowing that the transformer ratio appearing on the nameplate was incorrect.

Photos 4, 5 and 6 illustrate instances where the nameplate has been changed to report a turns ratio that is different from that recorded in the billing system.
1. Theft of Electricity

Photo 4 Current transformer with a changed nameplate (Example 1)

Photo 5 Current transformer with a changed nameplate (Example 2)
1. Theft of Electricity

Photo 6 shows a current transformer with a nameplate reporting a turns ratio of 200/5 (K=40) when, in fact, the transformer has a ratio of 300/5 (K=60). If this falsification was not detected, the customer would be billed for only two-thirds of the electricity actually consumed.

1.1.3 Loading Transformer

The most "professional" and "highly qualified" theft utilizes a “loading transformer”—a device created by the perpetrator that slows or stops the meter. A “loading transformer” requires some skill to construct, can be turned off and on to conceal the theft, and can be inserted into the secondary current circuit at any location that is exposed.

A “loading transformer” effects the theft of electricity by injecting enough current into the secondary circuit to negate the normal current from the current transformer and cause the meter to turn backwards. As a result, consumption is not recorded or is under-recorded. Typically, the current is injected into the secondary current circuit by jumpering across the circuit rather than by splicing into it, a method that is both easier to perform and harder to detect.
Diagram 2 outlines this method schematically. Photos 7 and 8 provide examples of load transformers.

Diagram 2 Use of a "loading transformer" to slow down a meter
1. Theft of Electricity

Photo 7 Single-phase "loading transformer"

Photo 7 shows a single-phase “loading transformer” that was used to rotate the meter backwards. A device such as this can be placed in a secondary current circuit at any location—close to the current transformer, near the meter, or on the line between the two.
1. Theft of Electricity

Photo 8 shows a three-phase "loading transformer" with the primary wire connected to a three-wire delta 380 / 220 Volts AC voltage source. The three secondary pairs of wire (coiled up in the photograph) from the "loading transformer" are jumpered across the three secondary current circuits. This loading transformer was confiscated from a site and taken to the Commercial Safety Department's office where it was photographed.

It is extremely difficult to detect this method of stealing electricity. First, only minimal tampering with the wiring is necessary and can be easily concealed. Even a very small exposure in the wiring is sufficient to insert the "loading transformer" and, to all but the most intensive inspection, the electrical network may appear to be in order and sealed. In one instance, the wire insulator had been pierced with a common sewing needle and that hole was used to connect to the secondary current circuit.

Second, "loading transformers" make it possible to reduce recorded electricity consumption gradually over time. That is, the meter can be rotated backwards periodically for several days and gradually but steadily reduce the meter’s record of actual electricity consumption, while also allowing the meter to go forward occasionally so that at least some usage is recorded. It is relatively easy to identify theft when the meter is stopped completely and consumption appears to be zero or near zero; these are good clues that something is awry and merits investigation. More sophisticated thieves slow the meter or allow it to rotate backwards periodically so that recorded consumption is, say, 30 percent below actual, a difference that is much more difficult to detect and may lend itself to legitimate explanations. Obviously, if
1. Theft of Electricity

perpetrators allow the meter to rotate backwards for a month or more continuously, the theft requires collusion with employees of the utility company who report the meter readings.

1.2 Secondary Voltage Circuit

Interfering with the secondary voltage circuit provides four ways to steal electricity. These include tampering with the voltage circuit wiring, removing or artificially damaging the fuses in the voltage circuit, opening the secondary voltage circuit, and cross phasing. Each of these methods decelerates or stops the meter so that electricity can be consumed without being registered.

1.2.1 Tamper with the Voltage Circuit Wiring

Voltage circuit wiring is often the focus of efforts to steal electricity, because this affects the ability of the meter to register electricity consumption. If the voltage breaker is not sealed (a common practice during Soviet times) it is very easy to manipulate the switches and steal electricity. Sealed voltage breakers hinder some of these efforts, but they can still be circumvented. For example, the seal’s hawser or hasps can be stretched so that the cover opens just enough to allow someone to insert a stick and switch the breaker off. The hole through which the hawser is inserted to seal the box also can be widened, again making it possible to manipulate the breaker with a long narrow stick. The latter approach can easily pass unnoticed without very careful visual inspection. Disconnecting voltage breakers can enable theft on a larger scale because several meters in the same substation can be stopped by opening the one voltage breaker on the voltage transformer that supplies the secondary voltage to several meters.

Diagram 3 outlines how the disconnection of a voltage breaker stops the meter from operating. Photo 9 shows a case in which the hole on the cover was widened to allow the insertion of a long stick, and Photos 10 and 11 are examples of unsealed voltage boxes that can be vandalized easily.
1. Theft of Electricity

Diagram 3 Disconnection of voltage transformer's breaker causes stopping of the meter

Photo 9 Enlarged hole in breaker box allows access to the voltage breaker
1. Theft of Electricity

Photo 9 illustrates how an enlarged hole allowed a customer to tamper with the voltage breaker. UEDC employees made the initial hole so that the box could be sealed tightly with a hawser. By enlarging the hole, the perpetrator could insert an iron stick and turn the voltage breaker on and off.

Photos 10 and 11 show how easy it is to connect and disconnect an unsealed voltage breaker.

Photo 10 Connection/disconnection of unsealed voltage breaker (Example 1)
1. Theft of Electricity

Photo 11 Connection/disconnection of unsealed voltage breaker (Example 2)
1. Theft of Electricity

1.2.2 Removal of Fuses in Voltage Circuit

Voltage commutation circuits (that is, secondary voltage circuits) can be artificially damaged such that electricity continues to flow to the enterprise but the meters fail to register usage or register only partial usage. For example, protectors (fuses) can be replaced by burnt protectors and the meters will not function. It is impossible to prove that this “damage” was inflicted for the purpose of stealing electricity; the simplest and nearly irrefutable explanation by the perpetrator is that the damage occurred during normal operations when the fuses burned out to protect the voltage transformer. Thieves may also remove the protector, which ceases operation of the electrical meter, but this practice is easily detected and typical only of less skilled perpetrators. Moreover, it does not matter if the fuses are on the high voltage (say, 10 kV) or the low voltage (0.4 kV) side of the voltage transformer. The ploy is equally effective either way.

Diagram 4 and Photo 12 illustrate this method of stealing electricity.

A       B          C                                 Voltage Tr.                                 Volt. Breaker                    Meter

Diagram 4 Replacement of working fuses (in red) with burnt fuses on the high side of voltage transformer causes incorrect metering
Photo 12 Deceleration of meter with burnt (open) voltage transformer's protector

Photo 12 shows three high side fuses protecting a potential transformer (PT) in a metering cubicle. The PT is in the cubicle on the right.
If a perpetrator cannot access the 0.4 kV voltage breaker at the metering point, it is possible to change the voltage transformer's high voltage side fuses. By installing a burnt high voltage protector - that is, introducing artificial damage - the meter rotation decelerates. Again, the burnt protector provides a good “cover” for the theft because the damage ostensibly occurred during normal operations (see Photo 12). If there is not a voltage transformer protector, perpetrators can use a simple wire instead of the fuse. (Use of a simple wire also violates published Georgian safety rules). Damaging or cutting one of the wires decelerates the meter (see Photo 13).

Photo 13 When high side fuses are absent, there is deceleration of the meter due to damage or intentional break in a wire

Sealing the voltage transformer’s doors, breaker and protectors makes it more difficult to access the fuses, but determined thieves overcome even these preventive measures. For example, perpetrators can remove the voltage transformer’s bus-bar during an outage of the 10kV system. Outages due to schedules (rolling blackouts), failure of the distribution equipment, or intentional downing of the 10 kV line by the customers make it possible to
1. Theft of Electricity

remove the bus-bar without great risk to the individual. Installing so-called “first standard (best) metering point” for customers apt to engage in this activity is preferred, but these measures are expensive. The “First standard (best) metering point” is described below.

1.2.3 Opening the Secondary Voltage Circuit

Opening the secondary voltage circuit and introducing a breaker is another method for stopping the operation of the meter. The voltage wires in Photo 14 were cut between the voltage transformers and the meter and subsequently reconnected to an improper triple breaker. The breaker appearing in this photograph was located in the customer's transformer kiosk between the wall and the floor, and the customer could start and stop the operation of the meter at will by manipulating the breaker.

Photo 14 Improper triple breaker in the secondary voltage circuit
1. Theft of Electricity

1.2.4 Cross Phasing

Altering or relocating current wires on the current transformers or untying the voltage wires causes meter deceleration. The number of wires altered or the nature of the modification affects the operation of the meter in different ways.

- If current wires are relocated on two of the three current transformers, the meter will rotate backwards.

- If current wires are altered on only one transformer, the meter will decelerate by two-thirds in the case of a symmetrical load (see Photo 15).

- Untying each voltage wire decelerates the meter by one-third. If two wires are untied, the meter decelerates by two-thirds; if all three wires are untied, the meter will stop. (Photo 16 shows all three wires untied).

To prevent this type of theft, current transformers should not be accessible to customers or they should be sealed thoroughly with clay and examined regularly for signs of tampering.

Photo 15 Deceleration of meter by cross-phasing

Photo 15 shows deceleration of the meter by altering "B" phase current wires. The clay seals have been removed from the "B" phase current transformer, and the current wires have been changed. This modification pulls back and slows the meter so that only one-third of consumed electricity is metered.
1. Theft of Electricity

1.3 Slowing the Meter

The methods discussed thus far enable theft of electricity, in large part, by slowing or stopping the meter by tampering with the secondary current or secondary voltage circuits supplying the meter. Electricity continues to flow into the household or enterprise but the meter itself is not powered. In this section, we discuss methods that involve physically tampering with the meter or its components. These include tampering with the discs or dials, affecting the meter’s performance by tilting it or placing strong magnets on it, and modifying or damaging the meter’s gears.

1.3.1 Dragging the Disc

The discs of the meter provide a means of stealing electricity in at least two ways. Physical contact with the top or bottom faces of the discs themselves creates friction and will slow or stop their movement. Materials also can be used to interfere with the rotation of the discs.
1. Theft of Electricity

Both approaches effect theft by slowing or stopping the discs and therefore registration of electricity consumption.

Photos 17 and 18 illustrate how direct contact with the discs can slow or stop the registration of electricity consumption. If the seal between the meter’s glass and the meter box itself is not tight, the perpetrator can insert a piece of photographic film through the opening. If the film can be pushed far enough to make direct contact with the display register or if it can reach the rotating shaft of the disc, the rotation of the discs will slow or stop. Photographic film is preferred because it is very thin, very tough, flexible in one dimension and rigid in the other dimension.

Photo 17 Mechanical effect on meter’s disk with photo film (Example 1)
1. Theft of Electricity

Photo 18 Mechanical effect on meter's disk with photo film (Example 2)
1. Theft of Electricity

Photos 19 and 20 illustrate a method that involves *holing* a meter and inserting a wire, stick, or other object across the rotating axis. The interference with the axis (or the disc itself) slows or stops the meter and electricity consumption is not recorded. We have discovered meters in which perpetrators have had to drill several holes, because the initial attempts were not aimed well enough to make contact with the rotating axis.

Photo 19 Holing the meter across the disk and mechanical effect on the disk (Example 1)
1. Theft of Electricity

Photo 20 Holing the meter across the disk and mechanical effect on the disk (Example 2)
1. Theft of Electricity

1.3.2 Tilting the Meter

The top and bottom bearings of an electric meter are designed with the expectation and requirement that the meter will be placed in a vertical position. Alternate positions cause drag or friction on the bearings and will affect the meter’s performance. Customers have learned to take advantage of this design feature and find ways to tilt or otherwise alter the position of the meter. Photos 21 and 22 show how perpetrators loosened the connection of the meter against the wall so that it is tilted or “hanging” by as much as a 90-degree angle rather than tightly affixed upright. The meter will decelerate or stop when tilted at such a severe angle.

![Photo 21 Laying a meter on its side to slow or stop its rotation (Example 1)]
1. Theft of Electricity

1.3.3 Strong Magnets

The proximity and strength of magnets will decelerate the rotation of a meter’s disc (and hence dials) by varying degrees. Photos 23 and 24 illustrate the placement of large magnets on a meter to affect its performance.
1. Theft of Electricity

Photo 23 Large magnets used to slow or stop the meter disc (Example 1)

Photo 24 Large magnets used to slow or stop the meter disc (Example 2)
1. Theft of Electricity

1.3.4 Tampering with Gears

The meter’s gearing mechanism provides a means to steal electricity by damaging or swapping out parts. If the teeth of the gears are sawn off, filed down, or broken, the meter will decelerate. Perpetrators also may swap out smaller gears for larger ones and, as a result, the meter will record less electricity than actually consumed. Photos 25 and 26 provide examples of gears that have been changed.

Mechanical interference with a meter’s gearing mechanism is not immediately obvious upon visual inspection. The meter’s discs continue to rotate and the apparent delays due to the interference (in mechanical meters as well as in electronic meters with mechanical displays) occur as the figures change or roll over. Specific tests and calculations based on the type of meter and consumed kilowatt hours are required to reveal the theft. When there is a varying load, detection is even more difficult.

Photo 25 Change of gear in metering point (Example 1)
1. Theft of Electricity

1.4 Tampering with Seals

Electricity is readily (and illegally) available to those who can remove and replace the seal on the meter. The seal itself does not prevent theft, but perpetrators who cannot replace the seal with a high quality forgery can be easily caught. Nonetheless, tampering with the seals on meters and metering points is a longstanding method of theft. In this section, we discuss methods for altering or falsifying seals as well as approaches that involve taking advantage of recertification procedures by government offices.

1.4.1 Falsification of Seals

Falsifying the meter’s seal is one of the oldest methods of stealing electricity. After opening the meter and altering its component parts or reducing the meter readings, the perpetrator must reseal the meter and do so with sufficient skill that the seal will not show obvious signs of tampering. The original seal itself may not prevent theft of electricity but evidence of a falsified seal is very strong evidence of intentional fraud and therefore UEDC investigators devote effort to expose these practices.

Falsification of meter seals varies based on the types of existing seals and their locations. Lead seals may be the easiest to forge because the sealing device can be duplicated. Among the highest quality devices neither careful observation nor expertise can detect the falsification. Corrupt employees of electricity distribution companies are, unfortunately, in the best position to assist in illegal activities. Employees with access to original sealing devices...
1. Theft of Electricity

can remove the old seals, replace them with new lead seals, and “age” the metal using vinegar or acid so that it appears very much like the original (older) seal. Even experts are unable to determine that the original seal has been replaced recently.

Although it may seem impossible to falsify a plastic seal, methods have been developed. A plastic seal must be twisted to complete the installation, and perpetrators have created a device that enables the opening and closing of the seal, and thus access to the meter. Visual inspection usually does not reveal tampering of plastic seals with such a device, but it can be detected with expertise.

Photos 27-32 illustrate falsified sealing devices, all of which are handmade.

![Photo 27 Handmade devices used for falsification of a certain type of seal (Example 1)](image)

Photo 27 shows devices that were extracted from the "Didi Navtlughi" substation when the theft of 1.3 megawatts (valued at 59,000 GEL or 33,000 US$) from the UEDC was revealed.

---

1 Average weighted wholesale tariff of 4.5 Tetri per kWh, and 1.8 Georgian Lari per 1.0 US Dollar.
1. Theft of Electricity

Photo 28 Handmade devices used for falsification of a certain type of seal (Example 2)

Photo 29 Handmade devices used for falsification of a certain type of seal (Example 3)
1. Theft of Electricity

Photo 30 Handmade devices used for falsification of a certain type of seal (Example 4)

Photo 31 Handmade devices used for falsification of a certain type of seal (Example 5)
1. Theft of Electricity

At the stage shown in Photo 31 the perpetrator drills out the inner red plastic with a drill bit (not shown).

![Photo 32 Handmade devices used for falsification of a certain type of seal (Example 6)](image)

Between Photos 31 and 32 the perpetrator alters the meter or metering in some way, then inserts a new plastic insert to the seal. In Photo 32 the perpetrator presses the new insert into the seal, leaving the impression that the seal has not been broken and reassembled.

1.4.2 Recertification by Government Meter Lab

Perpetrators of electricity theft have successfully involved the “Sakstandarti” (Georgian State Standardization Department) in ways that effectively “sanction” their activities and inoculate them from full penalties. For example, a customer might take his or her meter to the “Sakstandarti” periodically, such as once every three months. Before presenting the meter to the official, the customer removes the seals and downsizes the readings to the desired dial reading. The “Sakstandarti” should (and typically does) request a letter from the company on the regulation and sealing of the meter, but the customer declares that this meter is not to be used for calculations. Rather, he bought the meter himself and plans to use it only internally.

---

2 A customer might also have an arrangement with a corrupt “Sakstandarti” official who will not ask him to present a letter from the electric company.
1. Theft of Electricity

at his enterprise for his own recordkeeping. The “Sakstandarti” certifies and reseals the meter, issuing documentation to the customer as to these actions. The customer now possesses an official certificate as to the legitimacy of the meter, its seals and the meter readings at the time it was sealed, thus protecting him from charges of fraud or theft prior to that date. Even if UEDC employees subsequently discover illegal electricity consumption tied to that meter, the billing commission will be obliged to consider the Sakstandarti document of inspection and the corresponding time period. The billing commission can calculate and charge the perpetrator for illegally acquired electricity only for the period of time since the certificate was issued (say, three months) instead of a longer period, such as the twelve months permitted by Georgian regulations.

The fact that the customer owns the meter that is used by the utility for billing is a contributing factor to this problem. The UEDC has stopped the practice of the customer owning the billing meter. The practice of the customer owning the billing meter had been started long ago, before PA took over management of the UEDC.

1.5 Bypassing the Meter

Methods discussed thus far require some mechanism to decelerate or stop the meter from registering electricity. In this section, we discuss methods that involve bypassing the meter entirely. These include bypassing the meter at a switch and bypassing the meter with a concealed wire.

1.5.1 Bypassing the Meter at a Switch

Customers can acquire electricity illegally by holing the backside of the circuit breakers (switches) that are upstream of the meter and introducing an illegal line at that point. This method bypasses the meter at the switch, and the theft will not be discovered without lifting the current circuit breaker from its mounting. If the customer is aware of an impending inspection, the illegal activity can be suspended temporarily by taking the load from the illegal line. Diagram 5 and Photo 33 illustrate this method.
Photo 33 An illegal line taken from breaker before entering the meter

1. Theft of Electricity

Diagram 5 Illegal bypass ahead of the meter

1.5.2 Bypass the Meter With a Concealed Wire

Using an illegal line is the oldest and crudest method of electricity theft. It is possible to have an illegal line deliver the entire load, switching back and forth between legal and illegal lines.
1. Theft of Electricity

with a current circuit breaker. Or, an illegal line might be used to deliver only part of the electricity supply, for example to part of a building, only for heating, or only for kitchen appliances. Photos 34-37 provide examples.

It can be fairly straightforward to detect this type of theft when perpetrators take few if any steps to conceal their activities (see photos for examples). Alternately, employees of the Commercial Safety Department have encountered instances in which they had to destroy walls to reveal and remove illegal lines.

Photo 34 An illegal line connected to breaker prior to current transformers (meter)
1. Theft of Electricity

Photo 35 An illegal line taken directly from pole with a "fishing hook" (Example 1)

Photo 36 An illegal line taken directly from pole with a "fishing hook" (Example 2)
1. Theft of Electricity

1.6 Falsification of Meter Readings

Corrupt employees who are responsible for reading meters can assist in the theft of electricity. For example, an employee might underreport the electricity actually consumed by allowing a meter’s rotating discs to “turn over” to zero, catch up with the figures reported at the previous billing period, and surpass it by a much smaller amount than actually consumed. The new “false” reading is recorded and the enterprise consumes a very large amount of electricity illegally.

1.7 Meter “Doctor”

Finding and implementing new and innovative ways to decelerate electric meters has become so profitable and the services of skilled individuals are in such demand that it has become a profession of sorts. So-called meter “doctors” have fixed tariffs for their services, charging, according to our information, 10 percent of the value of downsized kilowatt hours for reducing meter readings in the UEDC network. We also have learned that the price of meter doctors’ services have almost doubled since the UEDC launched a widespread and intensive program to identify and prevent tampering with meters.

Unfortunately, the demand for meter doctoring and similar services can prove tempting to the employees of electricity distribution companies as well. Like meter doctors, employees of distribution companies like the UEDC and Telasi are compensated on a percentage basis for illegal activities. Out of the total bill for consumed kilowatt-hours, a customer might pay 30 percent to the company’s billing office and 35 percent to a corrupt employee of the company who can “fix” the books or in some way disguise the theft. The remaining 35 percent is not
1. Theft of Electricity

paid to anyone and is essentially net revenue to the customer (that is, electricity consumed but not paid for). We understand that similar tariffs apply throughout Georgia, with minor variations across regions and entities, and that they have increased over time as corrupt activities have become riskier. Prior to the UEDC’s anti-theft program, the corrupt employee could command only a 15 to 20 percent share and the customer received more than 50 percent net revenue.
2. THEFT OF INVENTORY

The UEDC’s anti-theft program focuses primarily on losses stemming from the theft of electricity. The scale and scope of electricity theft dwarfs other losses that the UEDC incurs due to diversion of materials, misappropriation of assets, etc. Nonetheless, the UEDC has addressed these areas as well and recognizes that efforts may be rewarded as much in discouraging unethical behavior on the part of employees or contractual partners as recovering lost revenue. Most instances of theft occurred before PA assumed management of the UEDC. Prior to PA’s management, little or no action was taken to investigate theft or punish perpetrators and managerial employees themselves stole or supported theft. Theft by employees has reduced significantly since PA began managing the UEDC; the Commercial Safety Department established by PA launched investigations, pursued legal action (submitting appropriate materials to law enforcement authorities), and initiated criminal cases.

2.1 Contractual Fraud

The UEDC has lost financial resources due to contractual fraud that was facilitated by corrupt employees. In one instance a group of perpetrators established a company and entered into a contract with the UEDC, agreeing to provide certain goods and services. Corrupt employees in the Technical Department certified that materials had been received and services had been performed, but, in fact, they had not. Another example includes transformers that were purchased by violating the rules of drafting the necessary documentation. The Commercial Safety Department revealed these and other instances of fraud and pursued legal and disciplinary actions as appropriate.

2.2 Diversion of Material

The UEDC has documented the diversion of a wide range of materials in varying quantities. Losses of equipment components, maintenance supplies, valuable metals, test devices, even vehicles (discussed in Section 2.3) and clothing have been discovered. At the Kutaisi Service Center, the UEDC investigated, and raised criminal charges, in a case that involved the misappropriation of 83,000 GEL to purchase copper and aluminum metals, transformers and special technical clothing. Dozens of such cases of varying scale and cost have been revealed at various locations.

One of the most egregious examples of diverting materials involved nearly seven tons of transformer oil. UEDC records showed the purchase of oil that was needed for routine maintenance and care of transformers. Documents also indicated (falsely) that the oil had been distributed to Service Centers and used appropriately by personnel to maintain transformers. In fact, an inspection of the transformers two years later suggested the oil had been diverted; it had been so long since the transformers had been serviced that nearly 150 tons of oil were necessary to perform required maintenance. Clearly, the transformer oil never reached the Service Centers or the worksites.

Dozens of such cases have been revealed but recovery of losses can be difficult. The UEDC recovered its financial losses at the Kutaisi Service Center after bringing criminal charges against the former Manager of the Service Center. However, in spite of the suspicious circumstances surrounding the loss of seven tons of transformer oil, it was nearly impossible to prove intentional theft and recover damages because the acquisition, distribution, and actual use of the oil had not previously been tracked carefully. The UEDC was successful
only in exposing Lanchkhuti Service Center’s former director for misappropriating materials since he signed off on papers accepting the (non-existing) oil but did not later register its consumption.

2.3 Diversion of Vehicles

The UEDC incurs losses due to the diversion and misuse of vehicles. This includes cases in which company vehicles are stolen and the perpetrators blame the theft on strangers as well as instances in which former employees, upon dismissal from the company, take a company car and refuse to return it. The UEDC is not always able to recover losses due to employee theft. Some perpetrators have close relationships with local authorities that protect them from prosecution; other former employees claim the losses stem from robberies that occurred during the Georgian civil war (1992 to 1994). The veracity of such claims, or lack thereof, is very difficult to prove.

2.4 Theft of Diesel and Petrol Fuels

In addition to stealing vehicles, perpetrators find ways to divert fuel for personal use. The UEDC investigators discovered company employees who were registering more mileage on company cars than were actually driven, thus receiving greater fuel allowances. An inspection of the Abasha Service Center, for instance, revealed that staff reported up to 35,000 additional kilometers that had not in fact been driven.

2.5 Leasing of UEDC Assets

The UEDC incurred losses as the result of convoluted terms and obscure clauses in legal forms that effectively hid the loss of assets. For example, a UEDC asset was leased (before PA) for a fairly modest fee but at the same time the contract required UEDC to reimburse the lessee for maintenance expenses. As a result, the lessee gradually appropriated the company’s asset (cash) and the UEDC continues to seek compensation or recovery of the material.

The UEDC (before PA) also entered leases for electricity transmission lines at usurious rates that inflict heavy financial losses on the company. The company is contractually bound by the terms of past agreements for lease or hire of certain assets that specified remarkably high prices as well as large penalties for non-payment of the leasing fee.

2.6 Falsified Receipts

The misappropriation of payments for consumed electricity is a widespread form of theft and one of the simplest to perform, but it is also the most difficult to investigate and resolve. The falsification of payment receipts takes different forms, but the sheer number of such instances (literally in the thousands based on our investigations) makes it extremely difficult to eliminate this type of theft.

Employees working for the company may create false electricity payment receipts and distribute them to customers. The customer pays the bill and receives the receipt but the employee pockets the cash. Alternately, the details of a paid receipt may be falsified such that only part of the payment goes to the company. For example, a receipt indicating payment of 500 GEL will be altered to show a smaller amount, say 100 GEL. The latter, smaller amount goes to the company and the employee keeps the balance.
2. Theft of Inventory

Combating theft by falsifying receipts was the focus of special attention by the Commercial Safety Department. The Department initiated twenty-five criminal cases involving falsified receipts and developed new procedures to prevent theft. For example, collecting cash payments was prohibited so that the cash collectors no longer had access to receipts; instead, customers received a receipt only from the company’s cashbox or bank upon payment of their bill. Special protective measures were taken in the preparation and production of receipts to further prevent falsification.
3. **ORGANIZATIONAL STRUCTURE OF AN ANTI-THEFT PROGRAM**

Facing theft and financial losses, the UEDC launched a program to combat theft of electricity and collusion by its employees. The program focuses mainly on theft of electricity rather than inventory or material, because unreported electricity consumption accounts for an estimated 80 percent of commercial losses. A Commercial Safety Department was established, protocols were created to conduct inspections, and priorities were developed to focus efforts on areas or activities that were likely to generate the most significant losses (that is, large amounts of illegally consumed electricity). At the same time, there was a renewed emphasis on professionalism, diligence, responsibility and basic integrity in the hiring and retention of staff in tandem with efforts to identify and resolve sources of corruption.

In this section, we first discuss the organizational structure that was developed as part of the UEDC’s anti-theft program. Then, we describe the types of policies and procedures that were established to support the actions of these departments. The next chapter discusses specific methods of detecting theft.

### 3.1 Commercial Safety Department

The UEDC established a Commercial Safety Department in March 2004 to spearhead the organization’s response to electricity theft. Initially employing only three individuals, the department grew to over 30 employees by January 2005 and included three subunits—the Energy Supervisory Service, the Technical Supervisory Division, and the Analytical Division. In turn, the Department’s Energy Supervisory Division is comprised of six regional services as well as a subdivision on supervising substations.

The divisional and regional structure of the department makes it possible to manage efficiently a large volume of work involving many different types of tasks across a widely ranging service territory. Each of the divisions focuses on specific tasks but coordinating their efforts is critical to the UEDC’s success against electricity theft.

#### 3.1.1 Energy Supervisory Service

The Energy Supervisory Service is the main locus of efforts to identify illegal electricity consumption at the points of distribution and usage. The service controls the accurate consumption and metering of electricity and is comprised of six regional services, each of which functions comprehensively in its corresponding territory. Employees inspect electricity acceptance and UEDC customers’ metering points to uncover attempts to gain illegal access to electricity using approaches such as those described in Chapter 1 of this report. To perform these activities efficiently across a broad range of customers and areas, the service established teams of employees within various regions and deployed them to conduct wide-scale inspections. Unified plans were devised for inspections so that three to five different teams could be operating simultaneously using the same protocol.

---

3 An all out blitzkrieg against theft would be extremely costly. Taken to an extreme, the costs of such an effort might even exceed the losses due to theft. The UEDC’s anti-theft program was designed to focus resources strategically on the greatest sources of loss while also establishing a level of effort and degree of vigilance that could be maintained over time.
Employees in the Energy Supervisory Service are authorized to draft formal documentation—Acts and Minutes of Administrative Offenses—when theft is discovered. These documents provide information for calculating the true electricity consumption (accounting for un-metered usage) and support the activities of the billing and realization departments to obtain estimates of commercial losses due to electricity theft and recover accurate amounts owed.

In addition to investigations of electricity meters and related equipment, the Energy Supervisory Service provides an important audit function and its inspections verify the effectiveness and honesty of the company’s employees. The Energy Supervisory Service examines the correctness of billing, the effectiveness of the billing system, and adherence to principles of operations management. For example, the staff confirms that customers are disconnected as appropriate if their accounts are in arrears, audits metering points to ensure that they are properly sealed and placed in order, and validates that the purchase of electricity is performed correctly. The service also reviews customers’ claims regarding electricity consumption, studies risk factors that may contribute to commercial losses due to electricity theft, and makes recommendations to reduce or minimize these risks.

### 3.1.2 Technical Supervisory Division

The Technical Supervisory Division focuses its anti-theft activities on the work of technical personnel and their compliance with safety regulations. The division examines the order of the network, inspects transformer points and communal re-metering to identify and remedy noncompliance with technical specifications that may facilitate electricity theft. In addition to reviewing the work of UEDC employees, the Technical Supervisory Division oversees the performance of contracting organizations. It inspects the timeliness and quality of contractors’ work as well as the validity of expenditures charged to the UEDC. In some cases, inspections by the Technical Supervisory Division revealed serious violations and contracting organizations were released from providing further services to the company.

The division is also responsible for investigating and preventing commercial losses from theft of inventory. For example, inspections conducted by the Technical Supervisory Division verify that purchased materials are utilized properly and that their use is correctly documented. Efforts by this division, in collaboration with the Analytical Division, uncovered falsification of transformer oil purchases in several Service Centers that totaled nearly seven tons of material.

Identifying potentially unsafe conditions is also a high priority for the Technical Supervisory Division. It verifies that correct procedures are followed as defined by technical safety norms, the law and company policy, and identifies noncompliant work that may contribute to dangerous conditions. This division advises technical personnel on risks and recommends work practices to prevent or minimize accidents.

### 3.1.3 Analytical Division

The Analytical Division performs critical support functions but also operates independently of the Energy and Technical Divisions. This division is responsible for shepherding cases of theft or corruption uncovered by the other organizational units through the legal system. It also engages in strategic planning by analyzing and prioritizing problem areas for the UEDC and recommending the type and location of surprise inspections.
3. Organizational Structure of an Anti-Theft Program

The Analytical Division conducts inspections across all phases of UEDC’s operations. The division often operates independently of the Energy Supervisory and Technical Supervisory divisions conducting surprise inspections on its own initiative as well as following-through on violations initially reported by the other two divisions. For example, the Analytical Division inspects cashboxes, examines the billing system and implementation of the billing sequence, and investigates issues related to writing off debts.

While technical experts staff the Technical Supervisory and Energy Supervisory divisions and undertake inspections of the electricity distribution and network infrastructure, lawyers make up the bulk of staff in the Analytical Division. These individuals conduct inquiries and prepare documents that support legal proceedings. The staff acts on behalf of the UEDC during the initial investigation of criminal cases and represents the company in any court appearances. The Analytical Division also maintains official communication with law enforcement authorities and supplies necessary materials to support legal actions in corruption cases and any other lawsuits.

3.2 Organizational Policies and Procedures

Along with organizing the Commercial Safety Department, it was necessary for the UEDC to establish systematic procedures and policies to support its anti-theft efforts. The UEDC designed and implemented procedures or systems for documenting and recording theft, equipped employees with standardized devices for testing, and established billing systems for the purpose of recovering losses.

- We implemented a special procedure in the form of an Act that was used to legally record theft and un-metered consumption of electricity.

- We established strict controls and registration of Acts to prevent corruption and collusive behavior.

- Ink stamps were devised to provide further protection and assurance as to the legitimacy of Acts, and only two such special stamps were produced for the company. As a result, it became impossible to perpetrate theft through corrupt measures such as tearing or replacing drafted Acts with false versions. Separate Acts were developed for single-phase and three-phase customers.

- A process was established for drafting Acts and authority was officially placed with some employees for their drafting. Specifically, employees of the Commercial Safety Department and Engineer-Technicians, who work on the network daily and are most likely to discover theft during the normal course of their work, were authorized to draft Acts.

- Employees were equipped with special diagnostic devices necessary to conduct tests and perform other activities. The devices were tested by “Sakstandarti” (Georgian State Standardization Department) and were certified to prove their validity. (Devices are to be re-tested each year.) Without a certificate, work performed with this equipment is not considered legal and cannot be used to support the drafting of Acts. The court could rescind the amount billed to the customer for alleged theft if the device used to detect and measure the theft is not certified annually.
3. Organizational Structure of an Anti-Theft Program

The UEDC developed protocols for recovering lost revenue after the theft of electricity had been documented. Information from the Georgian National Energy Regulatory Commission and other normative acts enabled the company to design and implement unified procedures for issuing acts and billing for recovery. The UEDC established Regional and Central Billing Commissions that determined the kilowatt-hours and amount of money to be billed based on each act. Preparation of materials necessary for the commission's work and coordination of their activities was performed by the Commercial Safety Department.

The UEDC developed formal standard operating procedures to be used upon exposing theft in tandem with changes in the existing legal framework. Electricity theft became administratively punishable according to the Code of Administrative Offences (that is, the Georgian penal code) and the GNERC adopted a corresponding decree at that time. The UEDC's standard operating procedures were published and became documents with strict registration procedures. The format, conditions, and rules for utilizing these standard operating procedures were defined throughout the company and issued to the regions.

3.3 Internal Audit Authority

While the bulk of its efforts focus on exposing illegal electricity consumption, the Commercial Safety Department also addresses losses due to the theft of inventory and diversion of assets.

The Commercial Safety Department thoroughly inspects all aspects of Service Centers, ranging from the center’s cashbox to its Technical Service’s Acts on Writing off Materials. These activities revealed instances of theft of cash, misappropriation and embezzlement of technical equipment/commodities, and so-called “immaterial operations”; that is, false purchase of materials and utilization of materials that are registered by the Technical Department but, in fact, never existed.

When theft or inappropriate use of materials is exposed, the Commercial Safety Department performs the necessary actions for recording the evidence legally (e.g., conducting internal inquiries, sealing material evidence and drafting acts). This evidence is then presented to the law enforcement bodies so that appropriate actions can be pursued.

3.4 Professional and Ethical Employees

Recruitment and retention of professional and ethical employees is essential to the UEDC’s program to expose and prevent theft. Not only is it necessary for the professional staff to have experience and be knowledgeable about the energy sphere, it is equally important that they have an understanding of legal issues and conduct themselves with unquestioned integrity and ethical behavior in their work activities.

Awareness of legal issues is important, because each investigation is fraught with a potential customer complaint that could undermine the claim or even bring legal action against the company. Any one instance of illegally restricting or infringing upon the customer’s rights could close out an investigation and, worse yet, call into question our entire effort by casting doubt on the legitimacy of our activities. Henceforth, UEDC activities and inspections might be tainted by the suspicion that customers were not treated fairly or that the company handled evidence carelessly.
3. Organizational Structure of an Anti-Theft Program

It is equally critical that the UEDC pursue all indications of theft, including those perpetrated by our own employees, and that it insist on the highest standards of work performance. Allowing corrupt or allegedly corrupt behavior to go unaddressed or unpunished would undermine our efforts to expose theft and insist that everyone “play by the rules.” The UEDC concluded that there were only a few cases in which the employees were, without a doubt, guilty of stealing or supporting the theft of electricity. More frequently, we identified situations where customers were illegally consuming electricity and the employee claimed they were unaware of it, lacked the proper measuring devices to detect the theft, etc. In the past, such excuses were left to stand; however, failure to recognize and report theft also causes commercial damage to the company and fosters a poor work ethic.

To strengthen its anti-theft program, the UEDC established a disciplinary policy to discourage negligent behavior on the part of employees. Henceforth, inquiries would be conducted of employees in charge who could reasonably be expected to know that electricity was being illegally consumed. Recommendations were made to the General Director as to the punishment in each case and, per the General Director, disciplinary action was taken. If the employee was undoubtedly involved in the theft, materials were sent to the law enforcement authorities for their review.

By establishing high expectations for employee behavior and performance, outlining and implementing a disciplinary program, the UEDC eliminated any notion among employees that they could act with impunity. The success of this program is reflected in the actions of employees themselves. Namely, it was only after this protocol was put into place that employees initiated requests to the Commercial Safety Department’s Energy Supervisory Division for inspection of a specific unit or a certain Service Center because the employee saw signs of illegal electricity consumption.
4. STRATEGY AND METHODS FOR IDENTIFYING THEFT

The UEDC’s Commercial Safety Department employs a variety of methods to investigate sources of electricity theft and minimize further commercial losses. While these methods continue to evolve as customers intent on stealing electricity devise new ways to acquire electricity illegally, we summarize the main approaches in this chapter.

4.1 Investigate and Study

Detailed study of the network is the primary investigative method employed by UEDC. This involves carefully analyzing the network at each Service Center, such as the number and type of customers that it serves, analyzing all points at which electricity losses could occur, estimating expected levels of consumption, and developing benchmarks. These activities are very labor intensive and require a dedicated and very detail-oriented staff, but they form an essential part of the anti-theft program.

To prioritize the allocation of staff resources, efforts focus on the Service Centers that have the lowest level of collections under the hypothesis that these Service Centers were experiencing the highest rates of theft. Staff analyze losses at every point in the network, ranging from the substations, feeders and transformers to the customers themselves. Service Centers where the analysis of aggregate data suggests something is awry are also early targets of careful study. For example, if Service Center “A” purchases electricity from two 110KV substations and the difference between the substation’s inlet meter and the total amount of the feeders is greater than that allowed by technical norms, un-metered electricity is being drawn from the network at some point. If the meters are in good condition technically, then it is most likely that manipulations are being performed on a feeder. Staff examine the situation, observe the units that receive electricity supply from these feeders or the transformers connected to them. Meter readings are taken and consumption loads are measured randomly, as well as systematically over time. These observations and analyses provide an estimate of the number of kilowatt-hours each feeder should be consuming and this figure can be compared with the unit’s official consumption.

These studies can be fairly straightforward when only one customer receives supply of electricity from the feeder. However, 90 percent of feeders provide electricity to several transformers, which, in turn, serve hundreds of residential and commercial customers. This feature complicates our study but the same principles apply. The investigative team develops a “short-list” of customers that might be stealing electricity or, at least have the strongest incentive to steal electricity (i.e., higher rates of consumption and therefore greater costs). Staff evaluate the number and type of customers served by the transformer, identify the units that likely have the largest consumption and determine whether they tend to operate during the day or at night. From the short-list, we identify which units and at what times it would be most productive to conduct an inspection. For example, if the short-list includes a bread factory, the unit should be inspected at night since bread is baked from 1:00am to 6:00am - those are the hours during which the factory will consume the largest amounts of electricity and the value (to the factory) of illegal electricity will be the greatest. The inspection itself proceeds in the same fashion as described above; investigators observe all aspects of the unit carefully for signs of tampering, employ measuring devices to determine if consumption is accurately metered, check all components of the primary and secondary circuits, all cables and cross pointing as well as locations where switches are installed (walls, floors, etc.).
4. Strategy and Methods for Identifying Theft

The initial review of the network sometimes generates a “short list” of potential perpetrators that is still fairly long or does not suggest a small number of very large consumers. When this happens, we cannot target resources efficiently to inspect a small number of units and the costs of pursing all metering points is prohibitive. Instead, we select a sample of metering circuits to inspect and conduct observations on the remaining customers to identify areas of potential illegal consumption that merit closer examination.

It is more difficult to determine how or where to focus investigative resources when the Service Center itself is stealing electricity. For example, Service Center “B” might reduce electricity purchase indicators by manipulating the inlet and feeder meters. As a result, the collection rates would appear to be higher than they are in reality or corrupt employees may find ways to monetize the un-metered electricity. When this occurs, it is impossible to assess the scope of potential losses solely through data analysis, because the aggregate indicators suggest the Service Center is fairly successful in collecting payments. Instead, staff develop benchmarks against which to compare levels of electricity consumption by identifying another Service Center with a similar customer base. For instance, Service Center “B” might have 10,000 customers, 500 of whom are commercial (i.e., three-phase consumers) and the remainder being residential (i.e., single-phase consumers). Staff compare Service Center B’s consumption with data from another, similar Service Center that shows no signs of falsifying purchase indicators. If the consumption rates differ significantly, the UEDC launches detailed inspections. Of course, the number of customers can be a faulty indicator for benchmarking data. Another Service Center with roughly the same number and type of customers might yield much higher or lower consumption simply due to patterns of use. Without a good benchmark, the best approach to investigating electricity losses at Service Center “B” requires careful observations of each customer and analysis of the installed capacity and consumption patterns. The time and personnel necessary for such work are very high and this method is used only in those instances where benchmarking data is unavailable or not credible.

4.2 Surprise Night and Weekend Inspections

Unscheduled night and weekend inspections are one of the most effective methods for identifying theft of electricity and deterring corrupt practices on the part of employees. Since customers generally expect UEDC employees to be working, and conducting inspections, during daytime hours, illegal consumption of electricity is more egregious at nighttime and on the weekends. Carefully planned surprise inspections afford UEDC staff opportunities to discover and investigate the widespread theft of electricity among its customers as well as at the Georgia State Electrosystem’s (GSE) transmission substations. In fact, several employees of the GSE were detained by law enforcement authorities based on the UEDC’s surprise inspections.

Surprise inspections also discourage collusive behavior on the part of UEDC employees. By conducting inspections at almost any time, including days and times that are not typically “working” hours, employees learn that there is no “safe” period during which they might assist someone in the illegal acquisition of electricity without risking discovery. Advance warning, or “leaks”, that alerted customers of an unscheduled inspection negated the success of some UEDC efforts and sometimes undermined plans that had been several days or even months in the making. Employees might do this not only for personal gain (for example, a payoff in exchange for the warning) but also to assist friends or relations. To address this problem, the UEDC implemented several unscheduled activities simultaneously. For example, one group
4. Strategy and Methods for Identifying Theft

of Commercial Safety Department employees might be performing analysis while a second
group conducted surprise inspections without any preliminary inquiry.

4.3 Thematic Inspections

The UEDC implemented so-called "thematic inspections", a practice that involves examining
similar types of customers throughout the company’s entire territory to provide valuable
information on patterns of electricity consumption among these different types of customers.
Hence, there were periods during which we investigated tea factories, then bread factories,
followed by stone processing plants, and so on across an array of types units. Following this
practice, several teams of UEDC inspectors simultaneously launched investigations of the
same types of units in different locations. These inspections yielded data on the
characteristics of work and electricity consumption in each type of unit and could be used to
benchmark consumption figures among units engaged in similar activities when we
suspected that official reports of electricity usage were unusually low.

4.4 The Government Standards Lab

In order to record legal manipulations to meters and seals, we implemented the practice of
using non-UEDC and non-Sakstandarti technical and legal experts, since at the initial stage
we could not trust "Sakstandarti (the organization dealing with the examination of seals and
meters). Our mistrust stemmed from previous experience in which the government lab
informed us of their conclusions that the seals and meters had not been falsified when, in
fact, there was obvious evidence to the contrary. In cases such as this, the UEDC does not
have any recourse - even a “second opinion” by an independent expert is worthless because
the evidence of falsification has been eliminated.

We presented this issue to the Bureau of Expertise at the Ministry of Justice—a move that
was unprecedented in the Georgian energy practice. By using the expertise of the Ministry of
Justice, we demonstrated to "Sakstandarti" that there was an alternative organization (the
experts at the Ministry of Justice) that could verify their actions. Subsequently, we requested
that they not conduct any inspections, not open any sealed meters, not inspect any seals or
other elements of the metering circuit without also having one or more UEDC representatives
present. In so doing, we made clear to UEDC customers and employees that opportunities
to gain a “favorable” (and false) conclusion from the expertise of Sakstandarti had been
eliminated.

4.5 Hardening of Electrical Network and Metering Installation

Sealing and hardening the electrical network, in combination with systematic inspection, was
an effective strategy when we suspected a facility’s official electricity consumption was under-
reported but we had been unable to expose the theft. Indicative of the success of this
strategy, the UEDC subsequently noted that official rates of consumption jumped by several
hundred percent at these enterprises and returned hundreds of thousands of GEL in revenue
to the company.

Sealing the network and metering installation complicates but does not prevent the theft of
electricity; that is, the perpetrator may still gain access to the system and acquire electricity
illegally, but it will be more difficult and require more time to remove signs of tampering.
Customers did not have time to cover-up signs of theft before inspectors arrived and UEDC
staff was able to record the unit’s actual consumption. Initially, inspections are conducted frequently to expose the theft and begin to establish actual consumption rates. Inspections can be conducted less frequently as we establish a stable pattern of typical electricity consumption for the unit.

4.6 Hardened 10 kV Metering Outfit

We created the UEDC’s “first standard metering cabinet” to reveal and prevent theft in the most difficult circumstances where the approaches outlined above were not effective. These situations usually presented additional and ostensibly deliberate efforts to obstruct our inspection activities. For example, the unit’s security service would not allow representatives to enter the area to conduct an inspection; the unit manager might hide the keys to the transformer point, or other obstacles would prevent our work from proceeding. These delaying tactics provided the perpetrators with sufficient time to conceal or eliminate evidence of electricity theft. Since the metering circuits were located on the private property of the unit, the UEDC could not, independently and without notice to the customer, investigate, detect, and identify the method of fraud at the metering. Rather, the UEDC could only cease the electricity supply.

For such entities, the UEDC created a “first standard metering cabinet”. The metering circuit is placed completely inside the cabinet, which, in turn is sealed and only meter readings can be taken from there. We used a special sealing method that was impossible to falsify. The method enabled us to place the seal on the door from the inside and it could not be reached without cutting the hawser. This procedure was quite expensive but it was cost effective in locations with large-scale theft of electricity where the UEDC recovered revenue that far exceeded the cost of implementation.
4. Strategy and Methods for Identifying Theft

Photo 38 "First standard cabinet" – Front view
4. Strategy and Methods for Identifying Theft

Photo 39 "First standard cabinet" – Oblique View
4. Strategy and Methods for Identifying Theft

Photo 40 "First standard cabinet" – 10 kV PTs secured and guarded

Photo 41 "First standard cabinet" – Close up of PT and CT Connections
4. Strategy and Methods for Identifying Theft

Photo 42 "First standard cabinet" – Back View; Panel Closed
4.7 Inspection of Neighboring Power Sector Companies

Although the UEDC focused most of its anti-theft investigations on its own customers, the activities of the Georgian Wholesale Electricity Market (GWEM) and Georgia State Electrosystem (GSE), and opportunities for illegal access to electricity by entities that GWEM and GSE dealt with, were also inspected. We discovered that UEDC employees sometimes worked in concert with the employees of the neighboring power sector company (transmission company, wholesale market customer, transmission licensee, etc.) to perpetrate fraud.

The analysis of feeders does not often disclose evidence of theft, but we discovered cases when so-called "subtracting meters" were used to steal electricity. If there were several feeders in the substation and even if the substation’s consumption was ideally balanced, we still checked the direct customers of GWEM. Opportunities for fraud arose because it was not unusual for a UEDC customer to receive electricity through customers of GWEM (that is, transit power). In this situation, the meter installed on the outgoing line (the "subtracting meter") was used to calculate the electricity consumption of the UEDC’s customer. The electricity consumed by the UEDC customers (metered on the "subtracting meter") was subtracted from the total amount of purchased electricity and the consumption of GWEM’s direct customer, which was metered on the feeder.
4. Strategy and Methods for Identifying Theft

The perpetrators - in this case involving employees of UEDC, GSE, GWEM, and customer employees - took advantage of this situation for personal gain. The meter installed on the line to the UEDC customer was intentionally accelerated. As a result, the apparent electricity consumption of the UEDC customer exceeded its actual consumption, and more electricity was deducted from the total amount in favor of (the other) GWEM customer. The latter, obviously, was gaining access to more electricity than for which it would be billed. Moreover, since the substation feeder was balanced, there were no obvious signs that anything was awry.

The UEDC has stopped the practice of using “subtracting meters.” Now all customer loads and feeders are to be directly measured with meters installed on the customer’s load and on the feeders.

4.8 Eliminating Illegal Lines

UEDC investigators used surprise inspections and unannounced outages to expose illegal lines that were not immediately visible. In many cases, customers routed illegal lines through underground cables that were not accessible to UEDC investigators because the cables were on private property or the size of the customer’s territory made a search impractical. Without careful inspection, the UEDC could not locate the switch between legal and illegal lines and provide evidence of theft.

To expose the existence of the illegal line, the UEDC secretly disconnected the legal line, thus presumably ceasing the supply of electricity. If the unit continued to receive electricity, it was clear that an illegal line was in place. This tactic was particularly successful among units that operated during night hours. It was somewhat more complicated to execute among units that operated during the daytime, but it was still done successfully. The most difficult cases involved those that relied on an illegal line for only part of their electricity supply—for example, for heating, kitchen appliances, or other uses that placed high demands on electricity. Here, the UEDC had to rely on surprise inspections and comparisons of metered kilowatt-hours and actual consumption to sleuth out the illegal line.

4.9 Detailed Inspections

Several types of violations can only be revealed by a detailed inspection of the network. These include falsification of transformer coefficients, tearing the contact on current and voltage wires, holing the meter, and hanging the meter. When we suspected these types of violations, we did not rely solely on inspections of the network using measurement devices since the theft might not be taking place at the moment of inspection. Rather, we examined the network carefully for a range of clues that suggested tampering. For example, by observing the connection points at voltage wires, we might observe that they were scratched, suggesting that electricity was being stolen by a “shunting method.” We paid attention to the thickness of dust on the meter and throughout the whole network. Meters were carefully checked by hand. We examined the outside of the meter to determine if it could easily be hung down, if the meter’s glass was unsteady or loose, or if there were residual signs of photo film on the meter’s disks. We even dissembled metering circuits and ceased the voltage supply to gain further clues as to the ultimate source and method of illegal electricity supply.
4.10 Checking Small Licensees

The UEDC discovered that electricity was being distributed illegally by small companies and by hydroelectric stations. Many of these operations had been in place for years, and it required considerable resources as well as legal action to cease the activity.

Small companies, so-called "small licensees" were distributing electricity throughout the territory of Georgia under license from the Georgian National Energy Regulatory Commission. The falsification of electricity purchase indicators raised significant revenues for these companies, and they frequently used UEDC’s transformers and lines as part of their operations. The UEDC inspected substations to reveal the nature and extent of the illegal activity and, in some cases, even resorted to disconnecting entire districts to expose the small licensees and their illegal use of UEDC infrastructure. The longstanding nature of these activities, often pre-dating PA’s management of the UEDC, made it extremely difficult to reveal the theft.

The GNERC has revoked nearly all of the licenses, and the customers and feeders have reverted to the UEDC.

We also discovered dozens of instances in which hydroelectric stations and various large enterprises illegally distributed electricity. These companies supplied electricity to nearby customers and collected electricity fees. Criminal charges were raised against these companies and the activities stopped after the UEDC collected and submitted material evidence as to the illegal distribution of electricity.

To further discourage illegal activity and develop positive working relationships, the UEDC entered into direct contracts with many of the small hydroelectric plans. Essentially, the contracts establish an agreement whereby the hydroelectric plants a) will not sell electricity “out the back door”; b) will allow UEDC to install advanced metering; and, c) will comply with the dispatch and switching orders of the UEDC, GSE, and GWEM. In exchange, the hydroelectric plant will be promptly paid the revenue due each month under the currently enacted GWEM Market Rules.

4.11 Use of Photographs

The UEDC uses photographs and video recording to provide supporting and incontrovertible evidence of theft. Customers often run away during inspections because they want to avoid signing the acts of investigation. With video recording equipment on hand, customers realize that they will be recorded on film if they turn and run. (In fact, the UEDC has a number of videos showing customers who were involved in theft that ran from the scene during the investigation.) The availability of photographic records allows the UEDC to avoid several lawsuits and support the company in winning cases against many perpetrators.

Investigators also use photographs to provide supporting evidence of suspected tampering, particularly the downsizing of meter readings. If earlier inspections and analysis suggest that the meter readings are being downsized, the UEDC staff identify the dates or times when such actions are most likely taking place. Several days prior to the anticipated time, staff inspect the unit and secretly photograph the meter readings. If subsequent inspection reveals that the meter reading has been reduced, investigators show the photographs of the earlier meter readings to the owner. Presented with this evidence, it is not possible for the customer to deny his illegal actions.
4.12 Improved Legal and Regulatory Framework

Our efforts to expose theft rarely go unchallenged by customers and the legislation in Georgia does not adequately address or regulate relations between the company and its customers. Indeed, the existing legal and regulatory framework may infringe on the company's interests through an imbalance that places excessive protection on customer’s rights relative to the utilities. It is particularly important, therefore, that UEDC employees exercise great caution in their investigations, document their work, and not become entangled in confrontations with customers. All employees are ordered not to respond to provocations, to take no action that heightens tension nor to do anything that could exacerbate a potential legal claim by the customer. There were cases where UEDC employees were threatened at gunpoint, but they were still required to remain calm and not become embroiled in an argument.

Cessation of electricity remains the primary tool available to investigators. The supply of electricity can be stopped to expose theft and to accumulate evidence for law enforcement authorities. Even so, there is no legal basis that permits the UEDC to halt the supply of electricity for an extended period of time.

The majority of inspections occur on the private property of customers, so it is not surprising that they take exception to visits by UEDC staff and have ample opportunity to hinder investigations. To overcome such obstacles, investigators have found ways to expose the obstruction and the theft. One such case required dividing the team into two, leaving one investigator to videotape (from neutral territory outside of the customer’s premise) the cover-up, while others were being held at the entrance by the customer using some delaying tactic.

In this case, the transformer point of the enterprise was located in the customer’s backyard, near a fence on the property line. Each time we attempted to inspect the transformer, the customer delayed the team for several minutes at the entrance. We suspected that they were entering the transformer point to conceal or eliminate evidence of theft before allowing us onto the property. In response, one member of the investigation team remained at the fence (off of the property) with a video camera; meanwhile, the rest of the team approached the main entrance and asked the person on duty to allow them to enter to conduct the inspection. The same situation unfolded; the security service held the employees at the entrance until such time as he obtained a permit from the enterprise’s director to allow them on the premises. Meanwhile, the customer’s engineering specialist went to the transformer building to eliminate any signs of theft at the metering point. The employee who remained behind, standing outside the fence, warned the engineering specialist that his actions were being recorded on videotape and that all materials would be sent to law enforcement authorities if he approached the transformer prior to our inspection. The engineer specialist became frightened and did not enter the building; upon our entry, we discovered that the enterprise had been stealing electricity by shunting the secondary circuit. Since the UEDC investigator warned the customer’s power engineer about the videotape, any defense based on “entrapment” was eliminated.
4. Strategy and Methods for Identifying Theft

4.13 Meter Seals

As described earlier, falsifying meter seals is one of the most widespread methods of stealing electricity. It is therefore essential to have seals that cannot be easily forged as well as policies and procedures that standardize their use. The UEDC implemented seals that were uniformly designed and could not be easily falsified, established procedures that controlled the use and installation of seals, and devised programs for tracking the use of seals—where, when, and by whom they were installed—that could be integrated with the billing system in ways that facilitated the recovery of lost revenue.

Before the UEDC implemented a unified sealing system, a wide variety of seals were in use and many of them could be falsified relatively easily. Each structural division selected and used their own choice of seals for the meters and elements of a metering point (that is, the current and voltage transformers, etc.). Lead seals that lack any identification marks were frequently used and this type was particularly vulnerable to forgery or corrupt practices because it lacked any kind of controlling feature (for example, a unique identification number). Even expert examination of such seals often cannot reveal falsification. The UEDC’s unified sealing system guarantees that only one type of seal is used throughout the company. Henceforth, any other type of seal is suspect. The UEDC selected a seal that requires twisting upon installation, has a numbered identification system, and includes protective devices that make falsification difficult and re-use (a second installation of the same seal) impossible. This type of seal is also the most cost effective.

The UEDC designed and implemented policies and procedures that govern the installation and removal of seals as well as appropriate record keeping for all actions involving placement and removal of seals. Prior to these actions, the company lacked not only control over the use of seals but also records as to who was doing what and when they did it. Only a few Service Centers could name the individuals who possessed sealing devices and no records were kept (at least not systematically) as to the date that units were sealed. As a result, the company was not always able to recover lost revenue. If a theft or violation had been revealed but it was impossible to determine the person who sealed the unit or the date that it was sealed, the Central Billing Commission could not calculate the incorrectly metered kilowatt-hours and issue statements for the correct amounts owed. Lack of records also made it impossible to pursue and correct inadequate work practices or corrupt behavior, such as poor quality seals or incorrectly installed seals that might have been done purposely to support the theft of electricity. Corrupt employees took further advantage of this situation by drafting an Act of Sealing with a favorable date (since there was no proof to the contrary).

The UEDC also initiated a special computer program to simplify control over the use of seals and ensure maximum accuracy of records. The program maintains a comprehensive registry and lists each seal in the company, its location in the region, its use at a unit, and, where applicable, its removal. A record of who used the seal, when, and why (usage, removal) is also kept. This program serves as another component in the company’s arsenal to protect against falsification and supports efforts to bill customers for lost revenue by eliminating ambiguities about the date and other characteristics of the seal when theft is exposed.
5. LESSONS LEARNED

The UEDC’s anti-theft program has nearly eliminated financial losses due to the misappropriation of material assets and illegal consumption of electricity has been substantially curtailed. However, important challenges remain. First, methods of theft continue to evolve. The UEDC has identified many of the different ways that customers steal electricity but the methods continue to proliferate in the hands of innovative and skillful perpetrators. Inspecting and investigating the means currently available to thieves remains a daunting task, let alone staying abreast of new approaches. Second, as the risk of electricity theft has risen, so too have the potential gains to those who can aid and abet this activity. Just as meter “doctors” can charge higher rates for their services, the rewards for corrupt activity may be increasingly tempting to employees in difficult financial circumstances or who are, for one reason or another, disgruntled with the company. Third, the disorder of the electrical network itself can make it more difficult to identify and resolve illegal consumption; equipment failure or network down time can create opportunities to vandalize or introduce mechanisms that will subsequently provide electricity to customers illegally.

The success of the UEDC’s efforts is reflected in the volume of cases that the Commercial Safety Department has processed. From its inception to May 1, 2006, the department has:

- Drafted 1,498 Acts of Theft and Un-Metered Consumption;
- Billed on 923 Acts amounting to 2,384,114 GEL in total;
- Brought additional income of 2,731,554 GEL to the UEDC after systematic controls on the metering and electricity supply of large customers was put in place;
- Submitted materials to law enforcement authorities on 162 cases based on the investigations conducted by the Commercial Safety Department's Analytical Division;
- Initiated 48 criminal cases;
- Issued disciplinary punishments to 442 employees, including warnings, reprimands, severe reprimands, and dismissals; and,
- Drafted 101 Acts of Violations as a result of inspections conducted by the Commercial Safety Department's Technical Supervisory Division, a division that started functioning about one year ago. The division also recommended specific actions to employees or groups and advised on disciplinary punishments when appropriate.

Furthermore, these figures understate the “true” success of the anti-theft program because they fail to quantify the impact of prevention and deterrence. We can offer “rough” indicators of the effectiveness of the program in this regard. For example, there are hundreds of cases in which Service Centers, upon learning that inspections were being conducted by the Commercial Safety Department, changed their behavior and began to record correct figures of electricity consumption. Similarly, we became aware of numerous corrupt arrangements that had been in place for some time but were severed by employees once they gained awareness of the repercussions if such schemes were discovered. We continue to investigate and record specific violations in such instances, but are also pleased that efforts to date are
5. Lessons Learned

discouraging corruption and reinforcing the importance of professional and ethical behavior on the part of UEDC employees.

Below, the main lessons learned from the UEDC’s activities are summarized, recognizing that the company’s efforts against electricity theft continue to evolve.

5.1 Organizational Structure and Strategy

- **Efforts to expose and prevent theft cannot be conducted effectively by a single sphere or department in the company.** To be successful, all aspects of the organization must be aware of, and involved in, the anti-theft program. This may require fundamental changes in the company’s human resources structure and attitudes towards its employees (e.g., specification of employee rights and responsibilities, improved working conditions, and rationalized policies governing wages and managerial decisions).

- **Anti-theft efforts include a range of activities that are efficiently organized into separate divisions or departments within the company, each with clearly specified roles and responsibilities.** For example, specific activities related to enterprise inspections or unit testing should be supervised by a special service or department that has been given the appropriate authority and the necessary material or technical facilities to conduct the work.

- **There must be close working relationships and full cooperation among all departments or divisions involved in the anti-theft program.** In the case of the UEDC, the various departments - Commercial Safety, Technical, Realization, Legal, and Human Resources - support each other in efforts to expose, substantiate, prosecute, and prevent theft. Left solely to its own devices, no single department or group will be nearly as successful. Moreover, the activities of each should inform and support the others. For example, methods of theft discovered by the Commercial Safety Department influence and improve metering and distribution standards and practices of the Technical Department. In turn, improved metering or meter seals less susceptible to tampering support efforts of the Realization Department to recover lost revenue.

- **Efforts to fight theft should be prioritized.** A company will quickly realize that fighting theft of electricity is a very expensive and complicated endeavor; begin with the simplest and least expensive methods. If and when theft continues, preventive measures should become progressively stricter (and probably more expensive). This approach allows the company to gauge progress and exercise control over expenses. It has the added benefit of possibly using recovered revenues to finance anti-theft activities; that is, initial returns from less expensive anti-theft measures can be reinvested gradually as the program succeeds to finance more expensive methods.

- **Anti-theft efforts must be constant and pursue all cases to their conclusion.** A company must call upon all possible ways and means to pursue each violation and win each case. Each lawsuit or dispute lost is apt to encourage additional theft or serve as a loophole for future perpetrators that utilize similar methods.
5. Lessons Learned

5.2 Policies and Procedures

- **Rules and procedures must be developed and codified.** Policies and practices concerning, for example, the ownership and use of seals, record keeping and reporting, expected codes of behavior and consequences for infractions are essential supporting material in the fight against theft. These materials often legitimate observed evidence (e.g., the paper or electronic record that matches the serial number on the meter) and deter corrupt behavior.

- **Procedures and documents that meet legal requirements must be developed, observed, and strictly registered.** These materials are necessary to ensure that evidence submitted to law enforcement authorities meet necessary requirements, support the overarching goal of fighting illegal behavior, and prevent destructive or corrupt actions.

5.3 Human Resources and Staffing

- **A professional and ethical staff is an essential core component to any anti-theft program.** Desired employee qualities (e.g., honesty, integrity, consistent work effort) should be communicated consistently and rewarded appropriately to encourage positive behaviors and discourage malfeasance.

- **Professional staff should be adequately remunerated to dampen the attractiveness of collusive or corrupt behavior.** Outstanding behavior and accomplishments of groups or departments - for example, milestones in the fight against theft - should be recognized to further encourage allegiance to the company’s goals.

- **Corrupt or collusive behavior must be dealt with swiftly and with appropriate severity.** Expectations and responsibilities of each employee must be clearly communicated, and infractions of company policies must not be ignored or addressed in a haphazard fashion. Clear disciplinary procedures should be in place so that the consequences of illegal or unethical behavior can be anticipated.

5.4 Methods of Detection

- **The metering and the sealing methods of the Soviet era must be abolished and replaced with modern methods that are less vulnerable to falsification.**

- **When the utility creates a new connection (that is, a new customer), the utility should install the meter and the metering outside the customer’s premises and at a location convenient to the utility company’s meter readers and inspectors.** For existing installations that are inside the customer’s premises, the utility may have to relocate the existing installation to a location outside of the customer’s premises.

- **The anti-theft program must continually evolve and adapt.** Methods for stealing electricity are not static; they continue to develop as perpetrators devise new and innovative ways to circumvent existing technology or exploit human weakness. An anti-theft program must regularly review its procedures, its organizational structure and relationships, its methods and decision-making processes to ensure that it is keeping pace with, if not ahead of, the activities of perpetrators. Just as UEDC
employees learn to recognize and anticipate the methods employed by thieves, so too do customers become accustomed to our methods of detection.

- **Modern technology, such as electronic meters, various seals, and other devices do not, in and of themselves, stop theft.** If not used wisely by the utility the new technologies may offer more opportunities for theft by the perpetrator. Careful analysis, intensive inspections, creative thinking, and diligent pursuit of all possible sources and explanations of electricity loss are indispensable tools in fighting theft.

- **Methods to fight theft are valuable for exposing existing violations as well as preventing future ones.** The preventive effect of anti-theft methods should not be underestimated.

### 5.5 Technical Designs and Field Practices

- **The meter and the metering should be both owned and controlled by the utility.** The customer should not own any part of the metering system.

- **The whole metering system needs to be sealed.** This includes the meter, the current transformers, the voltage transformers, all termination and junction blocks, and boxes containing the above items.

- **Meter seals should have unique serial numbers and their distribution must be controlled.** Written and signed records should be kept of which meter seals (by serial number) are issued to which employee. The utilities installation records (“paperwork”) for the metering job should indicate the serial numbers of the meter seals that were installed.

- **The tamper resistance and tamper evidence features of modern electronic meters should be turned “on” and used each month.** Modern meters have many features that aid revenue protection, but the features need to be in operation. More importantly, the features need to be read and used each month. Some of these features include load profile memory, detection of reverse power flow, times of power outage and power restoration, time of last reprogramming, and number of rests.