IOTA Papers

AN ANALYTICAL APPROACH TO DETECT MTIC/MTEC VAT FRAUD INVOLVING ENERGY TRADING

SO YOUNG KIM

NORWEGIAN TAX ADMINISTRATION

2017 December

IOTA
Intra-European Organisation of Tax Administrations

AN ANALYTICAL APPROACH TO DETECT MTIC/MTEC VAT FRAUD INVOLVING ENERGY TRADING

By So Young Kim

So Young Kim

Senior Tax Auditor

The Expert Group on the Cross Border VAT Fraud

The Norwegian Tax Administration

+47 9774 0415

soyoung.kim@skatteetaten.no

Introduction

Missing trader intra-community (MTIC) VAT fraud has long been the problem since 1993, with the creation of EU's single market. It has attracted increased attention throughout the EU, especially when the EU carbon credit market was severely hit by MTIC fraud in 2008 and 2009, which caused loss of more than EUR 5 billion for European taxpayers.[1] The fraud principally involves unfair competition, which threatens the entire market. The scale of the damage it can inflict is far beyond the revenue loss.

After carbon credit VAT fraud, it has been highly suspected that the energy market would become a target for fraudsters, mainly because of the similar characteristics

[1] https://www.europol.europa.eu/newsroom/news/carbon-credit-fraud-causes-more-5-billion-euros-damage-for-european-taxpayer

between the two markets.[2] These facts stress the importance and need of finding analytical measures to identify and prevent VAT fraud in energy trading. Through data analysis, the Norwegian Tax Administration detected two cases of VAT fraud occurred between 2013 and 2015 in the EU energy market.

This article aims to establish a better understanding of how the energy market functions in relation to MTIC (Missing trader intra-community) /MTEC (Missing trader extra-community) VAT fraud and provide a better idea of analytical approaches to tackle this issue.

Energy Trading

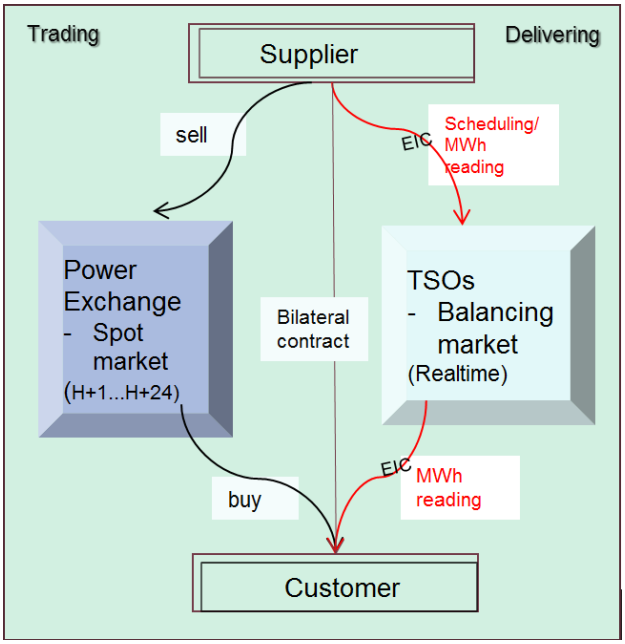
Energy is regarded as goods for VAT purposes according to number (19) of EU Directive 2006/112/EC, but unlike other goods, energy cannot be physically seen, touched or weighted. The coding scheme has been developed and used to organize the energy delivery in the EU internal energy market. This is to identify delivered amounts (MWh) and delivered parties (sender and receiver). Energy Identification Code (EIC) applies for all EU Member States.[3]

EIC code itself does not grant the right to trade energy. A market participant must be registered at national/local level according to each market rules. There can be several energy codes required when trading energy in EU.[4] These rules are also mandatory for non-EU market participants if they want to trade energy in EU.

[2] https://www.epexspot.com/document/19150/20111206-joint-statement-on-vat-fraud-prevention.pdf, https://www.entsoe.eu/fileadmin/user_upload/_library/events/130325_9_Associations_Press_Release_ENGLISH_FINAL.pdf

[3] www.entsoe.eu

[4] E.g. BDEW-code and EIC-code for the German electricity market; DVGW-code and NCG/Gaspool code for the German gas market



Energy disposition is obtained by declaration to TSO (Transmission System Operator), so-called via scheduling. It means when companies trade energy (Elspot) either bilaterally, via OTC brokers or power exchanges, they must deliver the traded energy through the grid of the TSO on the next day. Then, energy code is needed because the nomination is done through a web-based interface using EDI (electronic data interchange). In that sense, it can be said that companies only need a computer and internet access to carry out transactions.

Even though energy is treated as goods, it has functional characteristics similar to tradable services such as carbon credit, which makes it difficult to perform physical control. Then, a so-called "cyber physical control" can be performed on the data nominated at the TSO. However, the information is limited to the TSO national level and to volume data without price information.

Several European energy associations have taken market surveillance initiatives to implement REMIT (Regulation on Wholesale Energy Market Integrity and Transparency). Since 2015 ACER (Agency for the Cooperation of Energy Regulators) has operated the REMIT Portal as a centralized collection and storage of trading data, where all market participants are obliged to report their wholesale energy supply contracts with price information. ACER can monitor all transactions through this database.[5] It gives possibility for tax administrations to collect data and analyze mismatches between the traded energy and the actually delivered energy.

Relevance for MTIC/MTEC VAT Fraud

In EU, energy traded on the grid is subject to VAT where the customer is established with a reverse charge if the supplier is not established within the same country, cf. Article 195, cf. Article 38 and 39 of EU Directive 2006/112/EC. For EU VAT perspective, it is irrelevant in which country's energy market companies trade. Energy can be traded and physically stayed in one country while VAT fraud can be committed outside the borders of that country. It means the actual cross-border delivery of energy is not necessarily required to perform MTIC fraud.

[5] www.acer.europa.eu

Goods are not, theoretically, attracted to missing trader extra-community (MTEC) fraud, considering the role that the Customs play in the cross-border trade with a third country. Under EU VAT rules, energy is highly vulnerable also to MTEC fraud due to its characteristics explained above.

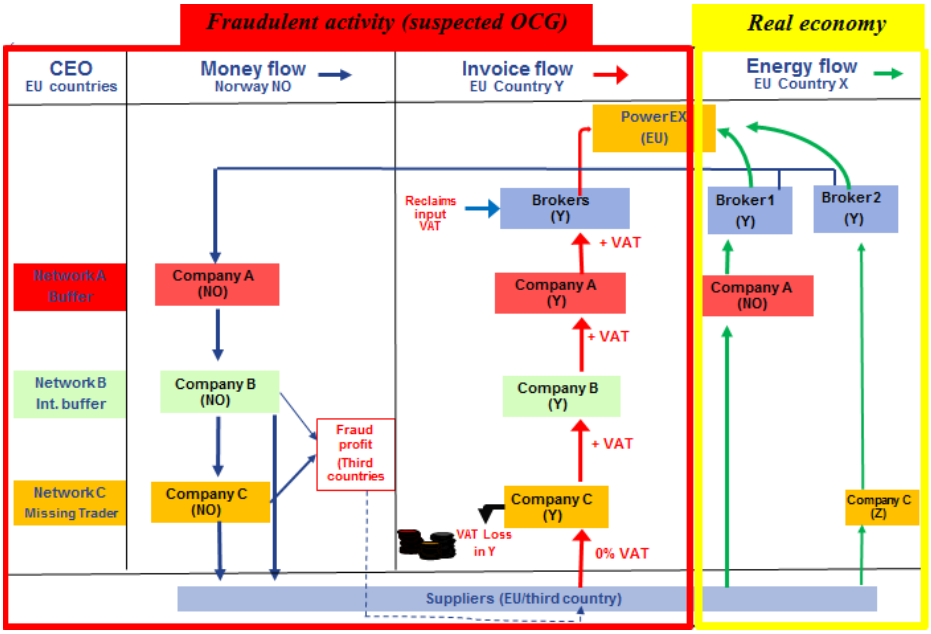
Energy can be traded cross-border within EU without having to be listed in the recapitulative statement, thus VIES data is not helpful for data analysis. It could be said that there is no harmonization between energy trading/physical delivery and VAT rules, which should be taken into consideration when implementing approaches of data collection and analysis.

Modus operandi

Norwegian tax administration detected two cases concerning VAT fraud in the EU energy market; one in electricity and another in gas. The electricity VAT fraud took place in 2013 – 2014 and the gas VAT fraud in 2015. Two Fiscalis Multilateral Controls were initiated and revealed the total VAT loss of approximately EUR 60 million. The two cases are committed by suspected criminal groups that have connection to the carbon credit VAT fraud.

The modus operandi of the electricity case is as follows:

- Establish a number of companies in several countries with foreigner as a director
- Trade electricity in EU country X where these companies have no residency
- Use false invoicing in EU country Y and money laundering in Norway
- The country X's electricity used for VAT fraud was controlled by foreign nationals domiciling in a third country, whom then used the missing trader in country Y to invoice the electricity delivered mostly by the Norwegian company.
- The VAT charged by the missing trader in country Y was collected from the brokers in the same country on onward sales and not paid to the tax administration in country Y.
- The brokers sold the electricity further to the power exchange in EU. When there are exchanges, fraudsters don't need to move goods round in a carousel, because they can simply buy again from the exchange.



The payment of the electricity trading was transferred mostly through the Norwegian bank accounts. The fraud profit, approximately 8 – 12 % of the total received payments, was then transferred to bank accounts in third countries. It is most likely to avoid all regulation by the countries of the companies involved. The ultimate destination of the profit is still unknown.

Analytical Approach

It is well known that criminal groups move quickly from one area to another (e.g. from carbon credit to energy), operating in different structures and forms. Then, it naturally requires tailored analytical approach. It is also observed that some roles of the criminal groups have some fixed patterns, which enables tax administrations to use predictable approach to some extent. Several analytical approaches have been used in Norway such as overall analysis, characteristic analysis, expert-based analysis and social network analysis. It is important to emphasize that these approaches are not separate, but complement to each other when applied in a combined action.

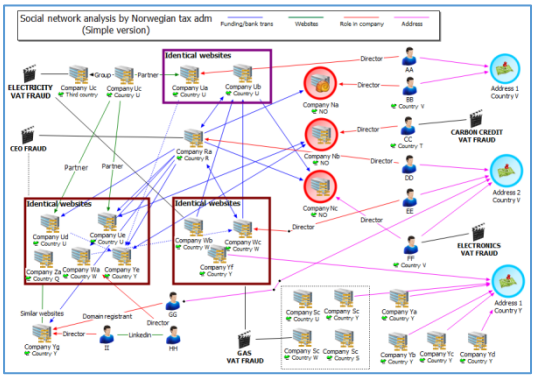
Overall market analysis is required to understand how the market functions and what data is available. The data sources used for energy analysis are: company register, tax administration's database, bank data, energy license data of the energy regulatory body, energy delivery data of TSO, and energy trading data of power exchange.[6]

[6] The possibility of using energy trading data from the REMIT was not considered since it was not ready when the Norwegian cases were investigated.

Once collected internally and externally from those sources, available data is interpreted and analytical approaches are defined to identify fraud indicators. The most successful approach is the expert-based analysis, which involves analyst's experience and business knowledge. Different models are built for different roles such as missing trader, buffer and broker based on the expert rules (risk indicators). Several refinements of indicators are conducted. The common indicators used for the energy cases are: newly established/off-the-shelf company, foreign director, address at office hotel, NACE[7] code for energy trading, VAT registration, large bank transactions without indication of business activity and no/minimal tax returns.

Each indicator is then weighted, and a risk score is calculated. Certain indicators are automated, e.g. director changes in the off-the-shelf companies, and consistently run against the data. The reliance on the risk score itself is not sufficient, thus this step is followed by manual scrutiny. When high risk is identified, it is important to monitor the identified objects on an ongoing basis, gather further data by exchanging information with other tax administrations/law enforcements and map the scope of possible fraudulent activities. Monitoring and early warning of identified risks could be time-consuming and extensive, but necessary to detect fraud.

MTIC/MTEC is often linked with organized crime, engaging multiple individuals, companies and countries. It involves often complex schemes in order to avoid tax administrations' radar. Social network analysis analyses contextual information around linked objects. It includes extra sources of information, not necessarily connected to a specific case. It is proven to be powerful approach to identify the fraudsters' next move.



The Norwegian approach is focused on the people behind the scheme and analysis of the relationships between objects. The variables used in the analysis are: websites of company, IP addresses, accommodation addresses, funding (bank transactions), links to other crimes, online social networking sites, energy code providers, web hosting services and third party company provider.

The analysis performed by the Norwegian tax administration was able to stop an ongoing VAT fraud involving electricity and gas trading. It further revealed the connections between carbon credit, electronics, electricity and gas VAT fraud as well as CEO fraud.

[7] http://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF