Guide on enhanced cooperation between Member States and Business in the field of fighting VAT fraud

EU VAT Forum
Brussels, February 2016
Contents
1. Introduction ......................................................................................................................... 2
  1.1. Purpose and context ........................................................................................................ 2
  1.2. Scope ............................................................................................................................ 3
  1.3. Stakeholders .................................................................................................................. 3
  1.4. Shortcomings of the measures currently in force to combat VAT fraud .................... 3
  1.5. Commitments of business and tax administrations ...................................................... 4
2. Commercial reality – Identifying and Managing Risk .......................................................... 6
  2.1. General aspects ............................................................................................................. 6
3. Normal KYC / KYT procedures ............................................................................................ 6
  3.1. KYC procedure (normal practice for business) ..........................................................7
  3.2. KYT procedures (normal practice) .............................................................................. 7
4. Exchange of information ...................................................................................................... 7
  4.1. Contact points in tax administrations for businesses ................................................ 7
  4.2. From business to tax administrations ......................................................................... 8
  4.3. From tax administrations to businesses ..................................................................... 8
  4.4. Between tax administrations ...................................................................................... 8
5. Use of data by tax administrations ....................................................................................... 9
  5.1. Tax administration must use the information received, must take actions .......... 9
  5.2. Feedback ..................................................................................................................... 9
6. Publicity and Follow-up (how the guide must be made available or implemented at national level, raising awareness) ................................................................................. 9
7. Guide updating ................................................................................................................... 10
8. Annex 1 - Description of the gas and electricity market .................................................... 11
  8.1.1. Background ........................................................................................................... 11
  8.1.2. The energy market ................................................................................................. 11
  8.1.3. General trading pattern and its relevance in the relation to VAT fraud ............... 12
  8.1.4. Registration according to REMIT ....................................................................... 13
  8.1.5. Balancing group and perimeter ......................................................................... 14
10. Annex 3 – Examples of “awareness” and “warning” letters ............................................. 20
  10.1. Awareness letter ....................................................................................................... 20
  10.2. Awareness letter (2) ............................................................................................... 23
  10.3. Warning letter (nominative) .................................................................................... 25
  10.4. Warning letter (2) ................................................................................................. 28
Guide on enhanced cooperation between Member States and Businesses in the field of fighting VAT fraud

1. INTRODUCTION

The VAT systems worldwide are increasingly complex and internationally interconnected. While the EU VAT system historically has been an inspiration internationally, the current EU VAT rules for cross border trade are known for their complexity and vulnerability to fraud and therefore exploited by fraudsters.

The increase in international trade and “new business models” driven by technological developments, such as (remote) services being supplied across multiple territories but also the increased use of outsourcing – including subcontracting - of supporting services/functions further accelerate the pressure on the VAT system.

The often huge differences and approaches in administrative practices of the 28 Member States also contributes to a system being highly complex and may have an impact on some of the processes mentioned in this guide.

As the VAT system is vulnerable to fraud there is a big need for a simple, fair, robust and efficient legal administrative framework in the EU and an efficient administrative cooperation process between Member States and with the legitimate business to prevent VAT fraud and combat it as effectively as possible.

1.1. Purpose and context

The purpose of this guide is to facilitate and encourage increased administrative cooperation between the stakeholders – see point 1.3 - endorsing this guide in order to effectively combat fraud without further complicating the EU VAT system. The guide will initially cover MTIC Fraud\(^1\) and its various mutations. As fraud schemes are constantly changing, the document could cover other types of fraud in the future. As this is a guide and not a binding agreement, it will support EU’s free market guaranties rules.

Fast and efficient dialogue and cooperation between tax administrations and legitimate business is essential when it comes to combatting VAT fraud. This guide on administrative cooperation between Member States and businesses particularly in the field of VAT fraud may help to encourage all stakeholders in the EU VAT system to use the guide as a basis for building effective cooperation models that can be built on as required.

This Guide should facilitate:

- a better and more pro-active interaction with legitimate business before new anti-fraud measures are introduced in order to evaluate impacts on legitimate business
- concrete actions to be taken by the various stakeholders on a pan-European level and nationally to share understanding of how businesses and markets operate, and to identify and jointly work on measures where the market is vulnerable to VAT fraud and thus foster timely and efficient cooperation.

---

\(^1\) As defined in COM/2004/0260 paragraph 3.2.2
• the implementation of these actions into national measures, through recommendations how this can be achieved
• increased development and exchange of best practices across the EU especially around cooperative compliance between legitimate business and tax administrations, know your counterparty-procedures (KYC) and know your taxpayer-procedures (KYT).

Sometimes business become facilitators in the loss of revenues by assisting the fraudsters unintentionally or without all the information needed to avoid this. Hopefully, this guide will ensure that the information required to minimise this risk as far as is possible, is made available to legitimate businesses.

1.2. Scope

The scope of this guide is to create a best practice framework for effective cooperation between tax administrations and businesses. The guide will also include more details of sound business models/practice in specific economic sectors (included in the annex) where fraud is a known problem.

1.3. Stakeholders

The stakeholders of this guide are listed on the EU Commission website and includes
• EU Commission
• Member States
• Tax administrations
• Individual businesses
• Trade associations

1.4. Shortcomings of the measures currently in force to combat VAT fraud

As well as enhancing conventional compliance responses over the last number of years, which quite often led to additional compliance obligations for legitimate business, the Member States have also been provided with additional tools to combat cross border VAT fraud e.g:

• The Eurofisc network (Council Regulation (EU) 904/2010 chapter X)
and
• The optional and temporary application of anti-fraud measures under the Quick Reaction Mechanism (EC directive 2013/42/EU) to fight sudden and massive VAT fraud and the extension of the domestic Reverse Charge Mechanism (EC directive 2013/43/EU) as a tool to stop VAT fraud in the first instance.

Several Member States have introduced sector specific reverse charge regimes over the last years, however, there are still no signs that the overall scale of VAT losses in the EU is diminishing significantly overall. Although a reverse charge is beneficial to the Member State to stop VAT fraud in a specific sector, it can lead to displacement of fraud to other Member States or into new markets, thus it does only cure the symptoms but not the root causes of VAT fraud. It is also not suitable for sectors vulnerable to non-compliance at the final or retail stage. It is also problematic and costly for legitimate businesses to keep track of the different reverse charge regimes applied in various Member States.
Work is underway to address the vulnerabilities to VAT fraud in cross border trade, such as the work initiated by the EU Commission on a final destination based EU VAT system but we also need closer cooperation between Member States as well as new approaches including greater involvement of legitimate businesses in terms of assisting in the fight against fraud.

1.5. Commitments of business and tax administrations

Measures to combat VAT fraud need to strike the right balance, by ensuring the safeguarding of VAT revenues while not increasing burden on legitimate business. There is also a strong need for efficient and timely international cooperation between Member States and between business and tax administrations. The specific commitments which arise out of this Guide seek to achieve these objectives while adhering to the fundamental principles and taxpayer/tax authorities rights inherent in the VAT system as follows:

- Legal certainty
- Neutrality
- Proportionality
- Transparency – mutual sharing of information

Business and tax authorities recognise that the commitments below are of mutual benefit and will serve to better protect all parties from the threat of MTIC VAT Fraud.
Joint Commitments
1. Businesses and tax authorities agree to share information which may assist in identifying and dealing with cases of MTIC Fraud (see Section 4). As part of this, the following principles apply:
   a. Businesses are encouraged to share commercial understanding and provide relevant information to the tax administrations on a timely basis (no matter if it is an ad hoc information request or during an audit procedure).
   b. Businesses and Trade associations are encouraged to warn as soon as possible the tax administrations of new patterns of fraud in certain economic activities that could distort honest competition.
   c. Tax authorities are encouraged to share information in the form of early warnings, fraud communications, sector fraud alerts, individual warning letters or other form of communications to businesses and trade associations (to the extent possible under local laws). Tax administrations are encouraged to provide information to other tax administrations on a timely basis (no matter if it is a spontaneous information or a request made during an audit procedure).

Business Commitments
2. Businesses are encouraged to increase focus when being informed of a known, specific risk and take commercially reasonable and available steps to ensure the adequacy of business processes, which have a bearing on MTIC VAT fraud e.g. KYC procedures (section 3), trade monitoring, segregation of duties, policy compliance review.

3. In sectors vulnerable to VAT fraud and being aware/informed of a known specific risk, businesses agree to take commercially reasonable and available steps to ensure that the awareness of MTIC VAT fraud is raised within their organisations and that sufficient training is employed for relevant staff.

Tax Authority Commitments
4. Tax administrations agree to increase focus as soon as becoming aware of a risk and put in place procedures to reduce fraud including taking reasonable and available steps to ensure the adequacy of processes, which have a bearing on MTIC VAT fraud, e.g. high standards to accepting taxpayers for VAT registration, KYT procedures, high level controls (early warnings), VIES³-data.

5. Tax administrations continue to ensure legal certainty for businesses committing themselves to this code of conduct and should offer certain commitment to use the information received only for the purposes of the guide for cooperation. Committing to this guide does not change the fundamental principles and taxpayer rights (such as presumption of good faith) inherent in the VAT system.

² See annex for example
³ VAT Information Exchange System
2. **COMMERCIAL REALITY – IDENTIFYING AND MANAGING RISK**

2.1. **General aspects**

Sound commercial understanding and an appreciation of how commercial aspects link into VAT in the business context is of the highest importance in order to be able to identify and manage MTIC fraud risks.

The relevant stakeholders mentioned in this Guide can only work efficiently and successfully together in the fight against VAT fraud if they fully and comprehensively understand the commercial reality, commercial drivers and the processes businesses have put in place to manage the environment in which they are doing business. This will facilitate a sound and reasonable assessment of what is commercially viable and expected within a sector, and what may indicate a fraud problem.

Business plays a key role in sharing information and actively helping to keep the tax administrations up to date regarding both the external commercial developments and the internal processes put in place by business to manage risk.

Business models are constant changing and the current marketplace requires business to constantly change and adapt to new business models. One thing that seems certain is that there will be more international trade across more territories. This will create further risks for business and challenges for tax authorities. Having a guide to help with the VAT fraud dangers will therefore become more relevant.

The annexes to the guide contain detailed guidance on certain economic sectors where the fraud has been and remains a particular problem. However, fraudsters can target virtually every economic sector so these are to be treated as examples.

Current sectors covered in details in the annexes in this guide are:

- The energy sector annex 1
- The Telecommunications sector, annex 2

3. **NORMAL KYC / KYT-PROCEDURES**

As part of the commitments within this Guide but also when it comes to managing VAT on a day to day basis, tax authorities and businesses recognise the importance of ‘Know Your Counterparty’ (KYC) and ‘Know Your Taxpayer’ (KYT) procedures in particular when it comes to the fight against fraud.

KYC and Kyt procedures should assess the standing of counterparties/taxpayers, using information that is reasonably available to businesses and tax authorities and would normally be included in the day-to-day processes. KYC and Kyt procedures are important at the start of a business or tax authority relationship, but also as part of the ‘in-life assessment’ of the ongoing relationships. Consideration should therefore be given as to how often KYC and Kyt procedures should reasonably be repeated.

Many Member States have already published guidelines in order to raise awareness of businesses as to what might indicate a potential MTIC risk. Tax administrations are encouraged to share information to assist businesses in developing their KYC procedures on an ongoing basis.
It is important to stress that when it comes to KYC and KYT procedures, there is not a standard KYC and KYT procedure for the entire business/taxpayer community. These procedures differ and need to be appropriate to the size, activity and type of taxpayer, and also need to take into account the volume and value of transactions as well as the number and type of suppliers and customers.

### 3.1. KYC procedures (normal practice for business)

In a business context, Know your counterparty (KYC) procedures are measures, which companies have adopted in order to reduce their commercial risk e.g. credit risk, reputational risks, corruption risks.

However, these procedures can also be an important element in the effort to minimise the risk of becoming unwittingly involved in fraudulent supply chains - even though it is important to be aware that good KYC-procedures cannot completely avoid this risk, given the sophistication and vast resources of the fraudsters and the constant change of fraud patterns.

Furthermore, it is also important to recognise that even where KYC has been performed, a “good” taxpayer can still turn/change its status from a “good” into a “bad” taxpayer over time or a fraudulent party could enter the supply chain of the business. It is not reasonable or commercially viable to expect a business to control or gain awareness of the counterparties with which its direct suppliers and customers are engaging. Ongoing alertness to the MTIC commercial risk indicators are recommended, which may indicate an issue once trading has commenced.

### 3.2. KYT procedures (normal practice)

Know your taxpayers are procedures put in place by tax administrations concerning for instance registrations and de-registrations. This requires specific processes and checks by the tax authorities. Adequate control and up-to-date communication through for instance VIES-systems is an essential element. It is encouraged that specific KYT-procedures are shared between Member States such as risk analysis/ risk management approaches, cooperative compliance regimes and taxpayer specific checks.

### 4. EXCHANGE OF INFORMATION

#### 4.1. Contact points in tax administrations for businesses

Tax administrations are encouraged to set up contact points on an international level (e.g. Eurofisc chair) and on a national level (in tax administrations in the Member States) for businesses, where they can directly share commercial information, i.e. how markets operate. It would be desirable to have permanent access through electronic means with this function. These contact points should be published.

To facilitate a fluent and easy exchange of information both parties, business community and tax administrations, should set up an efficient direct communication channel giving both sides the flexibility to act quickly and target oriented depending on the issue at hand. Where it makes sense as it increases efficiency and ease a single point of contact from each side could be appointed. Already today direct contact points are available to certain organisations in exposed sectors. Business associations could also be the contact point if necessary.
4.2. From business to tax administrations

Business and trade organisations should aim to organise sector specific workshops with tax administrations in order to share commercial background and spread relevant commercial information. However, as EU Competition law sets limits to the extent that businesses can share commercial information and whether they can actively monitor and act on open market movement of their products, any exchange of information would have to respect this legislation.

If there is suspicion of fraudulent traders in a specific market legitimate businesses are urged to pass on information to the tax administrations, provided competition law does not prohibit this.

Tax administrations are encouraged to establish an early referral process for business of suspicious trading patterns according to their national legislations, new market players or other irregularities identified during for instance the KYC/KYT-procedures.

The process should make sure that the exchange of information can be done swiftly and focused so that the information reaches the right team or group within the tax administration. Secrecy, confidentiality, free market guaranties should be taken into consideration by tax administrations when receiving data from businesses.

4.3. From tax administrations to businesses

The tax administrations are encouraged to publish guidelines which can help businesses to recognize risky business partners. Example includes postings on tax administration or sector specific websites. This will reduce the risk for businesses becoming an unwitting party to VAT fraud.

Tax administrations are also encouraged to establish an early warning process to business and business organisations, which can then spread relevant information further amongst the wider business community - "awareness" and "warning" letters. Examples of these types of letters are included in annex 3. Tax administrations do not have the possibility to inform businesses about specific companies suspected to be involved in VAT fraud due to secrecy law.

Member States are also encouraged to pro-actively consult with legitimate business before new anti-fraud measures are introduced in order to evaluate impacts on legitimate business.

Tax administrations shall swiftly react on relevant information received from businesses and take applicable measures as stipulated in section 4.1.

4.4. Between tax administrations

EUROFISC is a mechanism provided for the tax administrations in the member States to enhance their administrative cooperation in combating organised VAT fraud, and especially carousel fraud. (EU Council Regulation 904/2010) It is a network for the swift exchange of targeted information about VAT fraud between member States and a multilateral early warning system.

Eurofisc chair and national contact points in the MS are encouraged to be the contact towards businesses in relation to cooperation in this guide. Relevant information received from businesses could swiftly be shared with the tax administrations in EU through the Eurofisc network.
5. USE OF DATA BY TAX ADMINISTRATIONS

5.1. Tax administration must use the information received, must take actions

Tax Administrations often want to know commercially sensitive information about how a sector operates and they are encouraged to approach legitimate businesses who are best placed to provide such details, for example the relevant manufacturer of goods being targeted in the fraud.

Provided there is no business or contractual reasons restricting the provision of the required information, business will most likely provide the required assistance under the below mentioned assumptions and expectations:

- The representatives of businesses provide Tax Administrations with records and information on behalf of the business to the best of their abilities and in good faith. However, current representatives cannot reasonably be expected to have knowledge of all previous circumstances and matters referred to in the records and information provided.
- The Tax Administration will treat the information provided as confidential and accepts that the information will only be used for civil, administrative or criminal proceedings in question and the given information is not to be further disclosed or disseminated in any way whatsoever.
- Tax Administrations will discard the information once it is used or original intent is no longer required or relevant.

Tax Administration will request investigative assistance on a case-by-case manner. Information provided in an inquiry, cannot be assumed to be relevant or accurate to a similar in nature or resembling different investigative case.

5.2. Feedback

Although tax administrations cannot commit to give detailed feedback on how the information is used, they are encouraged to give an indirect feedback on what has happened with the information in general and what result has been achieved.

6. PUBLICITY AND FOLLOW-UP (HOW THE GUIDE MUST BE MADE AVAILABLE OR IMPLEMENTED AT NATIONAL LEVEL, RAISING AWARENESS)

For this Guide to be successful its consistent implementation both on an EU and national level is vital.

Therefore the following recommendations are given:

- The Guide should be endorsed by the EU VAT Forum and published on the EU Commission Website and we encourage all the Member States to publish it on their webpages
- Local and national fora and working groups (tax administrations, business organizations, businesses) should be established to promote its implementation and route back with its progress and experiences to the EU VAT Forum on annual basis.
- The guide should be distributed to business organisations, EU and national
- The Eurofisc network should actively promote the guide and the relevant contact points should be circulated to the relevant stakeholders

The opportunity to support the guide must be granted to all business and the relevant trade organisations.
7. GUIDE UPDATING

The effectiveness of the “Guide for enhanced cooperation between the Member States and Businesses” will be evaluated and future updates will be considered.
8. ANNEX 1 - DESCRIPTION OF THE GAS AND ELECTRICITY MARKET

8.1.1. Background

Europe's citizens and companies need a secure supply of energy at affordable prices in order to maintain our standards of living. At the same time, the negative effects of energy use, particularly fossil fuels, on the environment must be reduced. That is why EU policy focuses on creating a competitive internal energy market offering quality service at low prices, on developing renewable energy sources, on reducing dependence on imported fuels, and on doing more with a lower consumption of energy. This development is part of establishing the so-called European Energy Union.

The existence of a competitive internal energy market is a strategic instrument in terms both of giving European consumers a choice between different companies supplying gas and electricity at reasonable prices, and of making the market accessible for all suppliers, especially the smallest and those investing in renewable forms of energy.

There has been a strong drive for liberalization in the European Union energy markets starting back in mid-nineties and with further progression in the subsequent years. Accordingly, major legislative packages have been adopted in 1996, 2003, and 2009. These packets or programs were supported with the interest of increasing the interconnectedness and openness of markets to all stakeholders, i.e. producers, wholesalers, retailers, consumers.

8.1.2. The energy market

Energy, in particular electricity, is by its nature difficult to store and has to be available on demand. Consequently, unlike other products, it is not possible, under normal operating conditions, to keep it in stock, ration it or have customers queue for it. Furthermore, demand and supply vary continuously.

There is therefore a physical requirement for a controlling agency, the transmission system operator (TSO) to coordinate the dispatch of generating units to meet the expected demand of the system across the transmission grid (i.e. the bulk transfer of gas or electrical energy form generating gas and power plants to substations located near to population centers).

The scope of each energy market consists of the transmission grid or network that is available to the wholesalers, retailers and the ultimate consumers in any geographic area. Markets may extend beyond national boundaries.

---

4 See http://ec.europa.eu/priorities/energy-union/
5 The first liberalisation packet was adopted in 1996 (electricity) and 1998 (gas) with national implementation not later than two years after. The second liberalisation packet was adopted in 2003 and was to be transposed into national law by Member States by 2004, with some provisions entering into force only in 2007. The third liberalisation packet was adopted in 2009.
Roles of market participants

- **Producer**: a company that extracts gas or generates electricity.
- **Supplier**: a company that supplies gas or electricity to end users and needs transport capacity to do this.
- **Shipper (can be supplier too)**: a company that uses the national gas or electricity transmission grid to have gas or electricity transported based on a transport contract with Distribution System Operator (DSO).
- **Trader (wholesaler and retailer)**: a trade-oriented company that buys and sells gas or electricity at - sometimes virtual – market place for trading gas or electricity (hub). A trader does not necessarily have gas or electricity transported and does not always act as a supplier.
- **Consumer**: the actual user of the gas or electricity. A distinction is made between residential consumers (households and small businesses) and bulk consumers (businesses, industries).
- **Gas or electricity exchange operator**: a company that operates a gas or electricity exchange on the national or regional gas or electricity market.
- **Transmission system operator (TSO)**: the operator of the national gas or electricity transmission grid.
- **Distribution system operator (DSO)**: the operator of a regional distribution network.

If a producer, wholesaler, retailer or consumer wants to enter the energy market in a certain Member State, it has to register at the TSO of that Member State. If this participant also wants to be active on other national or regional markets, it has to register at the TSO in all those other Member States/regions. The requirements for registration at the TSOs follow the same pattern but may differ per Member State. Consequently, every TSO has a list with all the registered parties. However, this list is in some countries not always up-to-date.

Besides, the TSO lists sector specific rules (REMIT) also require all wholesalers to register at the European Register of Market participants (see further description below).

### 8.1.3. General trading pattern and its relevance in the relation to VAT fraud

There are significant differences in trading patterns between on the one hand the energy sector and on the other hand the vast majority of other industry sectors.

For example relates the VAT Fraud threat in the telecom sector mainly to the possibility of having little capital tied or uncomplicated technical setup to offer an Internet-based voice service (VOIP) or the fact that cell phones (mobile handsets) form small units, but with a high value which can be easily stored and moved around (well suited to 'carry out a carousel fraud'). In addition, these two areas are aimed at a broad group of end customers even for countries with a generally lower income base / purchasing power.

The same is not seen in the energy sector, where the same level of VAT fraud threat has not occurred. However, a few cases exist associated with the cheating party trying to engage in the wholesale market, as the retail market requires a more complicated arrangement setup with an electric or gas-distribution grid etc. Further, there is for the energy sector not a hardware based

---

6 For the sake of completeness, also companies – such as banks – are able to trade physically gas and electricity without having an agreement with a TSO. In these cases, such companies settle their commitments (positions) before physical delivery takes place.

7 Regulation (EU) No 1227/2011 on wholesale energy market integrity and transparency (REMIT)

8 https://www.acer-remit.eu/portal/european-register
threat, like when selling mobile phones. Likewise, electricity for example in its nature is difficult to store but must be delivered 'on demand'.

With the currently relatively low threat level that applies to the energy sector, the risk of cheating can be essentially further reduced by a robust KYC procedure. As mentioned above, in this context, the energy industry is also favored by a statutory registration with the common European energy authorities, Agency for the Cooperation of Energy Regulators (ACER), via national registration procedures. In addition, statutory records for the transport of electricity and gas at the respective TSO / DSO network operators are required. The risk of fraud is, thereby, limited principally to companies, which over time have had a normal wholesale trade before any VAT Fraud can take place. This requires a significantly larger capital bond, temporal extent and complexity prior to the fraud taking place. Consequently, fraudsters cannot just close a fraud company down for the day following rigging in another company name for the next day.

There is a distinction between 'exchange-based trading' and 'bilateral trading' / over the counter (OTC). Exchange-based trading is particularly widespread for trade with electricity, while trading in gas on a large scale takes place OTC, however, with a decreasing trend. Exchange-based trading requires an agreement with the exchange concerned regarding guarantees / collateral for completed transactions, etc.

OTC trades do not have the same formalities. Typically, OTC transactions happen with the same counterparty but from time to time, a new entrant enters. The latter requires usually a fairly comprehensive KYC procedure taking place. There are not yet rules for such KYC procedures, which therefore largely are based on each company's assessment of risks, ie typically credit risk by dealing with that counterparty.

Supervisory authorities are national energy and financial market authorities. Besides this, the supervision is monitored together with comprehensive Q&As, REMIT Transaction Reporting User Manual (TRUM) and guidelines made by ACER or European Securities and Markets Authority (ESMA).

There exists widely throughout EU a temporary reverse charge regime for electricity, natural gas and, in certain Member States, emission allowances, mainly as a preventive measure.

8.1.4. Registration according to REMIT

As of 7 October 2015 it has for wholesale gas and power companies become mandatory to register according to REMIT\(^9\). ACER Registration Code is used for REMIT transactions and orders reporting purposes.

ACER Registration Code within the REMIT Regulation compliance system means a numerical (alphanumeric, 12 values, example: 1234567890ab) wholesale energy market participant unique identifier assigned by the European Agency for the Cooperation of Energy Regulators (ACER) during the market participant registration process with the EU Member State National Energy Regulator (NRA).

No wholesale gas and power trading can take place without the counterparties being registered. Further, all trades are detailed reported under an unambiguous Legal Identifier Code.

Every system user that is connected to a gas or electricity grid (energy network) and is supplied from it or feeds gas or electricity into it must belong to a balancing group or form one of its own. Such a group consolidates wholesalers, retailers, generators, distributors and consumers into a (virtual) group, within which they can conduct commercial transactions in the energy market.

The users of each balancing group must choose a representative for their balancing group in charge of dealing with the TSO. The balancing group representative is responsible for the business management of their balancing group, maintaining the balance between inputs and outputs. Each grid input and output must be allocated to a balancing group.

By becoming a balancing group the participants can create their portfolio of business, which is referred to as their "perimeter". It is a kind of account. This balancing perimeter shows input from import, production and purchases on the market, and outgoing sales to consumers, the market and export.

The market is balanced within a certain margin. This is monitored by the TSO. If a market party does not respect this equilibrium it has to pay a penalty to the TSO (which is a percentage of the market price at the moment of imbalance).
VAT fraud scheme
After 7 October 2015 there are no longer, according to REMIT secondary legislation (COMMISSION IMPLEMENTING REGULATION (EU) No 1348/2014 of 17 December 2014)\(^{10}\), trading involving *unregistered* wholesale companies in the energy sector.

The VAT fraud scheme that took place prior to that date in the few known fraud cases (see hereunder) can hence no longer take place.

---

Background

The telecommunications sector is currently exposed to higher risks of Missing Trader VAT fraud (MTIC VAT Fraud) in the specific area of international voice wholesale, particularly VOIP. It is thought that this area of telecoms has been exploited by fraudsters due to the fact that it is relatively inexpensive and simple to set up a voice resale business, with limited requirements for office space and anything other than some readily available pieces of equipment and an internet connection. In addition, the sector is attractive to fraudsters as the business is fast moving and can generate high revenues in a short space of time, particularly when voice traffic is sent to high value destinations, such as Africa. In addition, due to the nature of international voice services, traffic can often be bought and resold many times, creating opportunities for looping of calls round the same set of counterparties several times.

In some countries, the telecoms sector is also exposed to higher risks of MTIC VAT fraud in relation to the trading of mobile handsets. The attractiveness of this to fraudsters in the past appears to have been as a result of the fact that these items are small but high value items, which can be stored or shipped relatively easily in order to carry out a carousel fraud. In more recent times, as far as the telecoms sector is concerned, the fraud now appears to favour intangibles which eliminate the need to deal with a physical product. Telecoms companies who are most at risk of being affected by fraud involving the sale of mobile handsets are those which buy from and/or sell to wholesalers of such items. In the case of large telecoms companies however, who may buy handsets directly from a manufacturer and sell on to retail customers, the scope for large-scale fraud to enter the supply chain is very limited.

In some countries which tax prepaid phone cards at the point of sale, there have also been carousel frauds in relation to the wholesale supply of such cards.

Other types of telecoms supplies, such as data services, content, SMS and national voice wholesale services are not currently thought to be a high risk from an MTIC VAT fraud perspective, albeit that general vigilance is required to identify any signs that the fraud may be moving into these areas.

This annex focuses on the risks attaching to wholesale voice transactions.

- Definitions

**International Voice Wholesale**- the buying and selling of voice services which originate and/or terminate internationally.

**VoIP**- Voice Over Internet Protocol is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analogue) phone line.

**Call Termination** – also known as voice termination, refers to the routing of telephone calls from one telephone company, also known as a carrier or provider, to another. The terminating point is the called party or end point. The originating point is the calling party who initiates the call.

**Call Origination**- also known as voice origination, refers to the collecting of the calls initiated by a calling party on a telephone exchange.
Destination – the country and operator to which the call is sent and the country in which the call ultimately terminates.

Carrier – a company that provides voice or data services. Carriers can be companies that operate wirelessly or over traditional wired land lines.

Reseller – a telecoms company without its own network, which resells voice, or other types of traffic.

Traffic – There are three types of traffic: voice, data and image, each with its own set of technical requirements for transmission.

Bilateral Agreement – Under this agreement, each party agrees to exchange traffic with the other party, usually with a commitment to exchange a certain volume.

Hubbing – the practice of providing or receiving worldwide termination services via a single interconnection agreement with a carrier.

Interconnect Agreement - An interconnect agreement is a business contract between telecommunications organizations for the purpose of interconnecting their networks and exchanging telecommunications traffic. Interconnect agreements are found both in the public switched telephone network and the Internet.

Switching - In a telecommunications network, a switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination.

ABP – Alternative Banking Platform, a virtual bank account which operates outside of the regulated financial sector.

Least Cost Routing (LCR) – a simple practice that finds the most inexpensive way to route phone calls. It is the process of analysing, selecting and directing the path of outbound and inbound communications traffic, depending on which path delivers the best rates.

- Market Participants.
- Tier 1 voice carriers – generally the largest, established carriers, who own and operate a national and international network, such as Vodafone, British Telecom Ltd and AT&T.
- Tier 2 voice carriers – generally smaller players, which operate in a similar way to the Tier 1 carriers, but rely on peering agreements with Tier 1 operators for some or all of their network access.
- Tier 3 voice carriers - voice resellers who do not have a network, but who buy and sell traffic from other carriers, routing that traffic via their own switching equipment.
- Telecoms Regulatory authorities, such as Ofcom. Please note however, that not all voice carriers are required to have a telecoms licence, depending on the type of services they supply, and the place of business establishment.
- Consumers – the actual user of the telecoms service, who either originates or receives a telephone call.
International voice wholesale is a very competitive market and it is not unusual for margins to be very low. Rates are usually set in US dollars at a price per minute and are likely to change on a daily, or even more frequent, basis. The market is largely driven by the two criteria of price and quality. All carriers will usually make use of a routing table which will identify the carrier to which certain traffic should be sent – in most cases this will be set to send the traffic via the least cost route, but other factors will be taken into account, such as whether there is a bilateral deal in place which should drive the routing decision.

However, in order to ensure quality, carriers, particularly Tier 1 carriers, will usually seek to send traffic via the most direct route possible, albeit this usually means paying a higher price e.g. if UK national carrier wishes to send traffic to Africa using a high quality route, it is likely to pass the traffic to an international carrier such as BICS or iBasis, who will then terminate the traffic directly with the relevant national carrier in the US. In such a scenario, the potential for Missing Trader VAT Fraud to enter the supply chain is very limited, if not impossible. By contrast, where price is the main driver of the transaction rather than quality, traffic originating from retail customers may pass through a number of resellers before reaching its destination. In such a case, there is a risk that fraudulent companies may become involved in these supply chains.

Traffic is passed from carrier to carrier via a network of cables and switching equipment. Telecommunications is exposed to a number of different types of fraud, such as false answer and international revenue share fraud. There are various methods employed by telecoms companies to identify such frauds and artificial traffic which may characterise some of those frauds. Supply chains involving MTIC VAT Fraud can often involve traffic which is, or may appear, genuine.

There are a number of currently accepted MTIC risk indicators for the telecoms industry, which are set out below. However, it should be noted that this is an indicative list of potential risk indicators, which should be complemented by general alertness to activity which looks unusual, or uncommercial. Businesses should take commercially reasonable and available steps to assess the existence of the below flags alongside any potential MTIC risk indicators identified as part of the KYC process.

It is however important to realise that many of the indicators are likely to occur within a normal wholesale telecoms relationship – what is important is assessing whether the risk indicator observed looks commercially reasonable in the relevant context. Particular care should be taken when risk indicators are observed for new entrants to the market, relatively new, or more established businesses which have had a change of ownership in a similar time frame, or where there are a number of inconsistencies and risk factors.
<table>
<thead>
<tr>
<th>Telecoms MTIC Risk Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Pricing, or other commercial terms which seem inconsistent with the rest of the market (seems ‘too good to be true’) e.g. minutes or handsets offered for sale below the open market value.</td>
</tr>
<tr>
<td>- Commissions or other kickbacks (e.g. gifts) being paid to suppliers or customers.</td>
</tr>
<tr>
<td>- Evidence of collusion with certain suppliers in setting prices such that each party in a supply chain may make a small margin.</td>
</tr>
<tr>
<td>- Evidence of supply chains being orchestrated e.g. unrelated companies agreeing or directing what amounts to invoice each other.</td>
</tr>
<tr>
<td>- Evidence of uncommercial (e.g. anti-competitive) conduct.</td>
</tr>
<tr>
<td>- Offers of, or requests for, loans or financing which appear unusual or uncommercial.</td>
</tr>
<tr>
<td>- Abnormal discounts, or deviations from normal values.</td>
</tr>
<tr>
<td>- Repeat deals at the same or a lower price and consistent profit, to the same destination.</td>
</tr>
<tr>
<td>- ‘Circular’ trading, in which the same wholesale capacity or mobile handsets are traded repeatedly among the same market participants, for a consistent margin or other evidence that the same supplies are being purchased or sold repeatedly.</td>
</tr>
<tr>
<td>- Revenue/Profit sharing arrangements.</td>
</tr>
<tr>
<td>- Unnecessary commercial steps inserted, inflating revenues.</td>
</tr>
<tr>
<td>- Identification/suspicion of other types of fraud.</td>
</tr>
<tr>
<td>- Flat trading profiles at all hours of the day and night.</td>
</tr>
<tr>
<td>- Offshore payment request (mismatch between counterparty location and payment location).</td>
</tr>
<tr>
<td>- Request to split payment of the net and VAT amounts.</td>
</tr>
<tr>
<td>- Payment date before invoice date.</td>
</tr>
<tr>
<td>- Requests for round sum payments.</td>
</tr>
<tr>
<td>- Other unusual payment terms.</td>
</tr>
<tr>
<td>- Mismatch between holder of the bank account for payments and the counterparty.</td>
</tr>
<tr>
<td>- Unexpected or inexplicable trading activity spikes.</td>
</tr>
<tr>
<td>- Unusually large amount of traffic with a counterparty.</td>
</tr>
<tr>
<td>- Unexplained or unusual quick changes in costs, revenues and traffic (quantity or direction).</td>
</tr>
<tr>
<td>- Rapidly expanding volumes of trade with either a counterparty or on a certain route, which does not appear to have a commercial explanation.</td>
</tr>
<tr>
<td>- Margins outside of normal commercial arrangements.</td>
</tr>
<tr>
<td>- Short gaps in invoice numbers.</td>
</tr>
<tr>
<td>- Trading thresholds exceeded.</td>
</tr>
<tr>
<td>- Request for payment terms that are shorter than normal.</td>
</tr>
<tr>
<td>- Looping of traffic or override of LCR principles.</td>
</tr>
</tbody>
</table>
10. ANNEX 3 – EXAMPLES OF "AWARENESS" AND "WARNING" LETTERS

10.1. Awareness letter

Belastingdienst

Belastingdienst, Post office box

Office

Address
Postal code RESIDENCE
Post office box
Postal code RESIDENCE
www.belastingdienst.nl

Team

Direct line
(088)

Subject: VAT (Carousel) fraud

Date

Our reference

Handled by

Dear Sir or Madam

For many years, the European Union has been hit by intra-Community VAT fraud (also called: VAT carousel fraud), in which the fraudulent trader does not pay VAT to the tax department, although he does charge and receive this VAT from his customers. The customers reclaim this VAT in their VAT returns, as a result of which -on balance- the treasuries of the EU countries suffer considerable losses. Despite a tightening of EU regulations and a number of anti-fraud measures in several Member States, it is not always possible to prevent the fraud.

**It has been established that at the moment a large-scale VAT Carousel fraud is taking place with goods, including mobile phones, tablets, laptops, game computers, action cams (e.g. Go Pro), SSDs and HDDs.**

I would ask you to provide an overview of all the suppliers and buyers you have traded with during the last 6 months. For the future, I also would ask you to report all the new suppliers and buyers prior to the first transaction to: (name official concerned).

By virtue of sections 47 and 53 of the General Tax Act (hereinafter: AWR) you are obliged to provide the tax inspector with data and information in relation to third parties (at his request). The way in which this is effected can be determined by the tax inspector (Section 49 AWR).
Due care
As an entrepreneur you must be careful when choosing your suppliers and customers in order to prevent becoming involved in e.g. VAT fraud. The Court of Justice in Luxembourg and other judicial authorities have determined several times that traders are expected to do everything that can reasonably be expected from them to prevent becoming part of a chain in which VAT fraud is committed. If you are not careful enough, you run the risk of being held jointly and severally liable for your supplier's tax debt in connection with the delivery of certain designated goods (see below, Section 42c of the Collection of State Taxes Act), or that your right to deduct input tax is revoked.

The fact that you exercised due care may appear from (among other things) the following:

- the way in which you got into contact with your suppliers and buyers;
- you have established that your contact persons are authorised to represent the companies;
- you can get into contact with these companies and their contact persons through the usual channels, such as a visit to the business address, a telephone number (landline) or a (recognisable) e-mail address;
- a comprehensive Know Your Customer procedure and the recording of the findings of this procedure for each new relation;
- extract from the Chamber of Commerce in which you can see what kind of company you are dealing with, if the company has been active in the sector, how long the company has been in existence, whether there have been recent changes in directors or shares, if the company employs staff, the company's address details, etc.;
- you know where the goods are at the moment of supply and you have the opportunity to have actual (physical) disposal of these goods;
- you check the goods yourself, or have a third party check the shipments;
- the goods are insured during transport;
- if the goods show defects, you can put in a complaint with the supplier.

The above enumeration is not exhaustive; you can demonstrate your due care in other ways as well.

As from 1 January 2002 Section 42c has been included in the Collection of State Taxes Act 1990. This section concerns the joint and several liabilities for VAT due, in relation to the supply of certain designated goods, for entrepreneurs who received supplies and who knew or should have known that the VAT due in relation to this supply was/will not be paid in full. These designated goods can be regarded as high-risk goods11.

In addition to the goods designated within the scope of joint and several liabilities, there are other goods of which it has been established that they are often traded in chains in which VAT (Carousel) fraud is committed. For instance (precious) metals, tablets, laptops, game computers, action cams, SSDs and HDDs and emission rights. High-risk goods are also mentioned on the website of the Dutch tax department under the heading Carousel fraud. Entrepreneurs trading in these high-risk goods must be especially alert to intra-Community VAT fraud.

You can ask the Netherlands Tax and Customs Administration whether the company you wish to trade with is known as an entrepreneur. If it concerns a company established abroad you can consult the EU site12 to see if the company has a valid VAT identification number.

You can also ask the Netherlands Tax and Customs Administration to help you with the precautionary measures you can take when choosing your trading partners.

---

11 Article 40a Implementing Regulations to the Collection of State Taxes Act 1990
12 ec.europa.eu/taxation_customs/vies/
If you trade in mobile phones, computer chips, tablets, laptops or game computers, you are obliged to apply the reverse-charge mechanism as from 1 April 2013, if this involves invoice amounts of €10,000 or more (excl. VAT) per type of goods per supply.

A commercial chain involving intra-Community VAT fraud often has one or more of the following characteristic features:

♦ it concerns trade in risky goods;
♦ it concerns cross-border trade;
♦ it concerns a chain of many companies;
♦ goods are traded in large transaction volumes, represent a high value and are sometimes offered below the common market price; this is often called parallel trade;
♦ it may concern goods alien to the business;
♦ suppliers and buyers within the chain change frequently, often involving new companies or restarted companies or companies with new managers/shareholders;
♦ others determine who you can/should purchase the goods from or supply the goods to. These ‘others’ can be your supplier or buyer, or an intermediary;
♦ it concerns trade with a high rate of circulation; purchased goods are usually resold immediately without keeping stocks; sometimes the supplier even indicates who the goods can be resold to;
♦ there frequently are cash payments and partial payments. It also happens that payments are made to persons, other than the suppliers;
♦ goods are usually stored at freight forwarders or transport companies and are not delivered to business addresses of the traders;
♦ supplies of shipments < €10,000, several similar supplies in quick succession.

If you suspect that you have become involved in an (intra-Community) VAT fraud against your will, you can report this to the BelastingTelefoon (Tax Information Line) as mentioned on the website of the tax department. If you have any questions or doubts, please do contact the officer mentioned below in this letter. Then it may be possible to prevent the fraud or to detect and tackle it at a very early stage.

Yours sincerely

Belastingdienst/……………

---

13 www.belastingdienst.nl
10.2. Awareness letter (2)

Dear Sir or Madam

I am writing to let you know that we believe fraudsters are making attempts to infiltrate the legitimate metals market in order to steal VAT through Missing Trader Intra-Community (MTIC) Fraud.

We are currently working with a range of businesses in this sector to raise awareness of MTIC fraud (see Annex A) and the co-operation and vigilance of those businesses involved in the metals trading sector will contribute significantly to preventing a potential attack. Given the increased level of risk, I would like to ask for your help in raising awareness of the threat with your colleagues within your business.

I appreciate that you should already have in place a range of corporate governance controls, which will include risk management checks when you do business with customers or suppliers. However, given this renewed threat, you may wish to review your existing processes and, if necessary, update your compliance, anti-money laundering and risk systems. As you will be aware, any business that knew or should have known that its transactions were connected with a fraud may lose its entitlement to recover associated input tax, so the consequences can be significant.

As part of your risk management process you may feel it appropriate to validate the VAT details of your counterparties. Details of how to do this are attached at Annex B. This may involve collection of more information and documentation about your customers and suppliers than in the past. As you no doubt appreciate we are unable to provide you with any authorisation or advice on whether to trade with specific counterparties; this will always remain a commercial decision for your business.

You can report to HMRC any suspicious activity in relation to VAT fraud online or by telephoning the 24 hour Customs Hotline on 0800 595 000

Yours faithfully,
Missing Trader Intra Community Fraud

MTIC fraud is a well-known and highly profitable criminal activity. This typically has involved ‘high value, low volume’ commodities imported VAT-free from EU member states. These are then sold in the UK, including a VAT charge, after which the importer goes missing without paying the tax due. Since its inception MTIC fraud has mutated and moved into intangibles and services in addition to the type of commodities mentioned above. (Although the term Missing Trader Intra-Community fraud has become widely recognised, it is important to note that in respect of services the same fraud can also be perpetrated by means of supplies received from outside of the EU. This is because the VAT rules for international services differ from those that govern supplies of goods.)

The following are examples of previous indicators of MTIC fraud and should be taken into consideration when conducting ‘Know Your Customer’ checks:

- Newly established or recently incorporated companies with no financial or trading history.
- Individuals with prior history of wholesale trade in ‘high value, low volume’ goods such as computer parts and mobile phones prior to the introduction of the reverse charge for those goods (June 2007) and/or carbon credits prior to their ‘zero rating’ in July 2009.
- Established companies that have recently been bought by new owners who have no previous involvement of trading in the metals sector.
- New companies managed by individuals with minimal experience and knowledge of trading in the metals sector.
- Companies whose business models are not suitable for, or compatible with, the trade of metals.
- Companies who make extensive enquiries about the VAT implications of trade in the metals Sector
- Inexplicable increases in the volume and values of trade in metals
- Unusual trading activity or arrangements that are incompatible with normal market behaviour
- Entities trading from short-term lease accommodation.

If you identify any of these fraud indicators you should consider the possible financial and reputational risks to your business before entering into a transaction.

HMRC Contacts

For further information on the metals sector threat please contact your Customer Relationship Manager (CRM), or contact the Customer Coordinators within HMRC.

In the event that you identify a potential fraud please contact the Customs Hotline on Tel: 0800 59 5000 or by accessing the HMRC secure website http://www.hmrc.gov.uk/customs-hotline/

In the event that you are unable to access this website, please write to the Customs Hotline using one of the following:

HM Revenue & Customs
Freepost NAT22785
CARDIFF
CF14 5GX, or

Email: customs.hotline@hmrc.gsi.gov.uk
10.3. Warning letter (nominative)

Belastingdienst

Belastingdienst, Post office box

Office
Address
Postal code RESIDENCE
Post office box
Postal code RESIDENCE
www.belastingdienst.nl

Team

Direct line
(088)

Subject: VAT (Carousel) fraud

Dear Sir or Madam,

I herewith inform you that our investigation has shown that you have purchased goods from (name supplier in question). Considering the circumstances, there is a strong suspicion that these goods are traded within a chain in which at least one party does not fulfil its VAT obligations and in which intra-Community VAT (carousel) fraud is committed.

I would ask you to provide an overview of all the suppliers and buyers you have traded with during the last 6 months. For the future, I also would ask you to report all the new suppliers and buyers prior to the first transaction to: (name official concerned).

By virtue of sections 47 and 53 of the General Tax Act (hereinafter: AWR) you are obliged to provide the tax inspector with data and information in relation to third parties (at his request). The way in which this is effected can be determined by the tax inspector (Section 49 AWR).

Due care
As an entrepreneur you must be careful when choosing your suppliers and customers in order to prevent becoming involved in e.g. VAT fraud. The Court of Justice in Luxembourg and other judicial authorities have determined several times that traders are expected to do everything that can reasonably be expected from them to prevent becoming part of a chain in which VAT fraud is committed. If you are not careful enough, you run the risk of being held jointly and severally liable for your supplier's tax debt in connection with the delivery of certain designated goods (see below, Section 42c of the Collection of State Taxes Act), or that your right to deduct input tax is revoked.
The fact that you exercised due care may appear from (among other things) the following:

- the way in which you got into contact with your suppliers and buyers;
- you have established that your contact persons are authorised to represent the companies;
- you can get into contact with these companies and their contact persons through the usual channels, such as a visit to the business address, a telephone number (landline) or a (recognisable) e-mail address;
- a comprehensive Know Your Customer procedure and the recording of the findings of this procedure for each new relation;
- extract from the Chamber of Commerce in which you can see what kind of company you are dealing with, if the company has been active in the sector, how long the company has been in existence, whether there have been recent changes in directors or shares, if the company employs staff, the company's address details, etc.;
- you know where the goods are at the moment of supply and you have the opportunity to have actual (physical) disposal of these goods;
- you check the goods yourself, or have a third party check the shipments;
- the goods are insured during transport;
- if the goods show defects, you can put in a complaint with the supplier.

The above enumeration is not exhaustive; you can demonstrate your due care in other ways as well.

As from 1 January 2002 Section 42c has been included in the Collection of State Taxes Act 1990. This section concerns the joint and several liabilities for VAT due, in relation to the supply of certain designated goods, for entrepreneurs who received supplies and who knew or should have known that the VAT due in relation to this supply was/will not be paid in full. These designated goods can be regarded as high-risk goods\(^1\).

In addition to the goods designated within the scope of joint and several liabilities, there are other goods of which it has been established that they are often traded in chains in which VAT (Carousel) fraud is committed. For instance (precious) metals, tablets, laptops, game computers, action cams, SSDs and HDDs and emission rights. High-risk goods are also mentioned on the website of the Dutch tax department under the heading Carousel fraud. Entrepreneurs trading in these high-risk goods must be especially alert to intra-Community VAT fraud.

You can ask the Netherlands Tax and Customs Administration whether the company you wish to trade with is known as an entrepreneur. If it concerns a company established abroad you can consult the EU site\(^1\) to see if the company has a valid VAT identification number. You can also ask the Netherlands Tax and Customs Administration to help you with the precautionary measures you can take when choosing your trading partners.

If you trade in mobile phones, computer chips, tablets, laptops or game computers, you are obliged to apply the reverse-charge mechanism as from 1 April 2013, if this involves invoice amounts of €10,000 or more (excl. VAT) per type of goods per supply.

A commercial chain involving intra-Community VAT fraud often has one or more of the following characteristic features:

- it concerns trade in risky goods;
- it concerns cross-border trade;
- it concerns a chain of many companies;
- goods are traded in large transaction volumes, represent a high value and are sometimes offered below the common market price; this is often called parallel trade;
- it may concern goods alien to the business;

\(^1\) Artikel 40a Uitvoeringsregeling invorderingswet 1990.
\(^*\) ec.europa.eu/taxation_customs/vies/
suppliers and buyers within the chain change frequently, often involving new companies or restarted companies or companies with new managers/shareholders;

- others determine who you can/should purchase the goods from or supply the goods to. These 'others' can be your supplier or buyer, or an intermediary;

- it concerns trade with a high rate of circulation; purchased goods are usually resold immediately without keeping stocks; sometimes the supplier even indicates who the goods can be resold to;

- there frequently are cash payments and partial payments. It also happens that payments are made to persons, other than the suppliers;

- goods are usually stored at freight forwarders or transport companies and are not delivered to business addresses of the traders;

- supplies of shipments < €10,000, several similar supplies in quick succession.

If you suspect that you have become involved in an (intra-Community) VAT fraud against your will, you can report this to the BelastingTelefoon (Tax Information Line) as mentioned on the website of the tax department. If you have any questions or doubts, please do contact the officer mentioned below in this letter. Then it may be possible to prevent the fraud or to detect and tackle it at a very early stage.

Yours sincerely,

Belastingdienst/………………

---

16 [www.belastingdienst.nl](http://www.belastingdienst.nl)
10.4. Warning letter (2)

FAO The Director
Tel
Fax
www.hmrc.gov.uk

Date
Our ref
Your ref

Dear Sir,

Re: Tax losses linked to Sales by you to XXX Ltd in VAT period xx/xx

HMRC have been making enquiries into transaction chains which may be linked to Missing Trader Intra-Community (MTIC) fraud. As a result of these enquiries we have been made aware that supplies/a supply made by you to XXX Ltd in (month) are/is part of a transaction chain(s) leading to a taxable person in another EU Member state that fraudulently defaulted on its tax obligations after the supply was made to it by your company / a company in your transaction chain.

I must however point out that checks are still ongoing in the aforementioned period (s) with a view to gathering further supporting documentary evidence.

Your sales invoice(s) found to be connected to the tax loss is/are listed below:

<table>
<thead>
<tr>
<th>Invoice</th>
<th>Date</th>
<th>Manufacturer</th>
<th>Model</th>
<th>Quantity</th>
<th>Unit Price</th>
<th>Total</th>
</tr>
</thead>
</table>

You should be aware of the following ruling(s) by the European Court of Justice (ECJ). [Delete the sections(s) below which do not apply. In particular, please ensure that you do not refer to Kittel if the trader is not claiming input tax (e.g. if the reverse charge applies).]

- Input tax recovery of VAT should be denied where the person claiming input tax either knew or should have known that his transaction was connected with the fraudulent evasion of VAT. This principle, known as the Kittel principle, has been clarified and endorsed by the Court of Appeal in the UK and is not limited to a connection with fraud occurring in the UK.
• Zero rating for an intra-community supply should be denied where the taxable person has failed to fulfil his obligations as regards evidence, or the taxable person knew or should have known that his transaction was part of a tax fraud committed by the customer, and that he had not taken every reasonable step to prevent his own participation in that fraud. This is the principle known as Mecsek.

• The ECJ judgment in the case known as Italmoda ruled that a taxable person who knew, or should have known, that a transaction relied on as a basis for rights to deduction of, exemption from or refund of value added tax, was part of a chain of supplies connected with the fraudulent evasion of VAT, may be refused the benefit of those rights, irrespective that the evasion was carried out in a Member State other than that in which the benefit of those rights was sought.

The issue of this letter is without prejudice to any future action that HMRC may decide to take in relation to your right to recover the VAT incurred and / or zero-rate the above transaction(s). [Remove the reference to recovery of VAT if the trader has not claimed input tax on the corresponding purchase(s)]

You should satisfy yourself that you have the requisite evidence to support zero rating for supplies made to overseas customers and taken all reasonable measures to ensure your company’s transactions do not lead to your involvement in transactions connected with the fraudulent evasion of VAT.

You should satisfy yourself that you have undertaken sufficient due diligence commensurate with the perceived risk to satisfy yourselves as to the integrity of your suppliers and customers, and of the underlying supply chains.

It is your responsibility to determine which checks to carry out and whether to undertake transactions in light of the results of those checks. Examples of checks that you may wish to consider are listed in Notice 726 – Section 6 (enclosed).

For the avoidance of doubt I should finally tell you that this letter is without prejudice to any enquiries HMRC may be making on any other transactions which you have already been involved in and which may be in a chain of transactions where VAT has gone unpaid.

If you wish to discuss this letter or have any further enquiries please do not hesitate in contacting me.

Yours faithfully,