5-3-2013

Stopping MTIC – With a 3rd Invoicing Directive

Richard Thompson Ainsworth

BU School of Law

STOPPING MTIC – WITH A 3RD INVOICING DIRECTIVE

Boston University School of Law Working Paper No. 13-13
(May 3, 2013)

Richard T. Ainsworth
Boston University School of Law

STOPPING MTIC – WITH A 3RD INVOICING DIRECTIVE

Richard T. Ainsworth

A Third Invoicing Directive for the EU VAT seems to be a foregone conclusion.[1] Corrections are needed in the current (and newly adopted) Second Invoicing Directive, but the hallmark of the next Directive will almost certainly be its application of digital invoice technology.

Based on the critical commentary offered on the Second Invoicing Directive,[2] it is reasonably clear that a Third Directive needs to be crafted.[3] This paper is directed at that effort, but is not simply directed at "corrections."

When the Commission proposes a new Directive, the proposals will surely include adoption of tax-technology advances in invoice-control that are currently in use outside the EU. It is reasonably clear that the next Invoicing Directive should require comprehensive e-invoicing, invoices that are digitally signed, and invoices that are fed into a system of relational databases that match transaction data across the Single Market. There will be real-time EU sales/purchases lists, and remote/real-time audit functionality.

This will occur, because the true target of the Third Invoicing Directive will be missing trader intra-community (MTIC) fraud, not invoices. Improvements in invoicing will be a means to achieve a larger end.

[1] Following a study [PriecwaterhouseCoopers, *A Study on the invoicing Directive (2001/115/EC) now incorporated into the VAT Directive (2006/112/EC)* of November 3, 2008] and a public consultation on invoicing [launched by the Commission on July 24, 2008 and summarized in the report of November 2008 (TAXUD/DI/GW/mve D(2008) 25115] the EU Commission Proposed a Second VAT Directive on January 28, 2009 [COM(2009) 21]. On March 16, 2010 the Council of the European Union reached agreement on the Commission's proposal and formally adopted the Second Invoicing Directive on July 13, 2010 [Council Directive 2010/45/EU 2010 O.J. (L 189) 1].

[2] See: Gorka Echevarria Zubeldia, *The Second EU Invoicing Directive: A Missed Opportunity*, Nov./Dec. INT. VAT MONITOR 417 (2010) (itemizing how the Second Invoicing Directive has fallen short on its promise of simpler and more harmonized rules in invoicing); Patrick Wille, *New EU Rules on Invoicing*, Jan./Feb. INT. VAT MONITOR 6 (2011) (discussing simplified invoices, cash accounting and the continuing requirement that customers control the use of e-invoices); Isabelle Desmeyiere, *The Hidden Features of EU Invoicing Directive 2010/45*, Nov./Dec. INT. VAT MONITOR 400 (2011) (explaining how new rules on the chargeability of VAT in instances where the related invoice has not been issued will lead to complexities when States exercise differing options, and the complexities that may result from further development of the cash accounting option); Joep J. P. Swinkels, *Confusing EU VAT Invoices from 2013*, May/Jun. INT. VAT MONITOR 174 (2012) (explaining how the large number of official languages in the EU and the compulsory clauses on invoices may cause confusion particularly in cases where a small business under cash accounting sells to a larger business).

[3] This might occur by 2017, as paragraph 24 of the Second Invoicing Directive (replacing the current Article 237) indicates:

> By 31 December 2016 at the latest, the Commission shall present to the European Parliament and the Council an overall assessment report, based on an independent economic study, on the impact of the invoicing rules applicable from 1 January 2013 and notably on the extent to which they have effectively led to a decrease in administrative burdens for businesses, accompanied where necessary by an appropriate proposal to amend the relevant rules.

This will not be a "black swan" IT effort.[4] The needed technology is here today; the necessary systems are tried and proven in large multi-jurisdictional tax systems; the implementation costs will be a small fraction of the €100 billion that is currently lost to MTIC fraud annually.[5]

This paper begins to "connect the dots." It considers Brazil's successful digital invoicing regime in the *Sistema Publico de Escrituracao Digital* or Public System for Digital Accounting (SPED)[6] and applies what has been learned there to the pattern of MTIC and missing trader extra-community (MTEC) frauds in the EU.[7] A follow-up paper will align the Croatian *Fiskalizacija – IT* (Fiscalization program)[8] with the Brazilian SPED, and then consider the data security and remote audit functionality of the newly implemented Rwandan system.[9]

[4] A "black swan" is a term coined by Nassim Nicholas Taleb to describe high-impact events that are rare and unpredictable but in retrospect seem not to be so improbably. In an IT context research shows that there are a surprisingly large number of out-of-control tech projects. *See*: Bent Flyvbjerg & Alexander Budzier, *Why Your IT Project May Be Riskier Than You Think*, September HARVARD BUSINESS REVIEW (2011); Richard T. Ainsworth, *Technology, VAT Compliance, and "Black Swan" Blindness*, 66 TAX NOTES INT'L 275 (April 16, 2012).

[5] Europol, *SOCTA (Serious and Organized Crime Threat Assessment) 2013 – Public Version*, 27 (March 2013).

[6] SPED contemplates replacing paper tax and accounting books and documents with electronic versions where legal validity is confirmed with a digital signature. Once a firm begins to issue NF-e invoices, or CT-e electronic waybills paper replicas of these documents are not legally valid. Digital documents are given legal precedence over paper replicas. *See*: Newton Oller de Mello, Eduardo Mario Dias, Caio Fernando Fontana & Marcelo Alves Fernandez, *The Evolution of Electronic Tax Documents in Latin America,* PROCEEDINGS OF THE 13TH WORLD SCIENTIFIC AND ENGINEERING ACADEMY AND SOCIETY (WSEAS) INTERNATIONAL CONFERENCE ON SYSTEMS (2009) 449, 297, *available at*: http://dl.acm.org/citation.cfm?id=1627575&picked=prox; and Newton Oller de Mello, Eduardo Mario Dias, Caio Fernando Fontana & Marcelo Alves Fernandez, *The Implementation of the Electronic Tax Documents in Brazil as a Tool to Fight Tax Evasion,* PROCEEDINGS OF THE 13TH WORLD SCIENTIFIC AND ENGINEERING ACADEMY AND SOCIETY (WSEAS) INTERNATIONAL CONFERENCE ON SYSTEMS (2009) 449, 453, *available at*: http://dl.acm.org/citation.cfm?id=1627575&picked=prox

[7] MTEC is a variant version of MTIC fraud. MTIC occurs in goods, and relies on the reverse charge mechanism whereby cross-border business purchasers of goods self-assess the VAT. Rather than self-assessing and remitting the VAT due fraudsters sell the goods in the domestic market, and collect VAT (which now becomes part of the profit margin). The same reverse charge procedure applies in B2B service transactions, but in this case the services need not be supplied by a business within the EU. Services supplied from third-countries to EU taxpayers are subject to the reverse charge, and when these services are "tradable services," like VoIP, CO2 permits or various technology products sold through the Internet, the same MTIC pattern is replicable as MTEC. See: Richard T. Ainsworth, *VAT Fraud: The Tradable Service Problem*, 61 TAX NOTES INT'L 217 (January 17, 2011).

[8] *See*: the official Croatian tax authority web site where all information about "fiscalization" can be found and updated regularly http://www.porezna-uprava.hr/fiskalizacija/fiskalizacija.asp; Republic of Croatia Ministry of Finance Tax Administration. [Republika Hrvatska Ministarstvo Financija Porezna Uprava], *Fiscalization program* [*Fiskalizacija – IT*] (in Croatian) powerpoint presentation *available at* http://www.hgk.hr/wp-content/files_mf/Fiskalizacija_HGK_v0.3.pdf.

[9] Rwanda Revenue Authority, Electronic Billing Machine, *available at*: http://www.rra.gov.rw/rra_article1035.html

Brazil's tax modernization program includes an Electronic Invoice, or the *Nota Fiscal Eletrônica* (NF-e)[10] and an Electronic Waybill, or the *Conhecimento de Transporte Eletrônico de Cargas* (CT-e).[11] The NF-e and the CT-e are the centerpieces of the SPED program. These digital documents have similar functions, the NF-e is for transactions in goods, and the CT-e is for inter-state transport of those goods. Once a business begins to use NF-e and CT-e for inter-state transactions it must use NF-e and CT-e for all transactions (intra-state and inter-state).[12]

Brazil's digital invoicing efforts stretch back to September 15, 2006 when it began the NF-e pilot project. Progress was rapid. By April 2009 there were 25,000 NF-e issuers. The CT-e pilot project began October 25, 2007. It involved two states (São Paulo and Rio Grande do Sul) and 43 companies and transportation firms. By March 1, and April 1, 2009 respectively the firms in Rio Grande do Sul and São Paulo began issuing legally binding CT-e documents. Large-scale adoption of the CT-e began in 2010, and by the end of 2010 there were over 500,000 firms issuing digitally signed, cross-border NF-e invoices. The system is fully in place today.

Aspects of the Brazilian SPED are replicated in Croatia and Rwanda. All three jurisdictions have been driven to digital invoicing in their efforts to stem tax fraud. Croatia and Rwanda are focused on business-to-consumer (B2C) frauds; Brazil is concerned with cross-border business-to-business (B2B) fraud. In each instance the essential solution is the same – fraud prevention follows from data security and transmission of this data to a central server. The oversight is real-time.

There is much to be learned and borrowed from these systems. Workability is assured. It is only a matter of time before the EU fully embraces digital invoicing, and the Third Invoicing Directive is the opportune moment. The reason for it is clear – at €100 billion MTIC fraud is getting far too serious to ignore, and a new Invoicing Directive can solve it.

This paper first considers the Brazilian SPED, and the cross-border tax fraud it prevents – "invoice sightseeing," also known as *nota fiscal fria* or "cold invoice." It then sets out the development of the EU VAT Information Exchange System (VIES) and the MTIC frauds it was designed to prevent. It is important to see this development because the VIES in some respects is a prisoner of its direct tax ancestry.

Subsequent papers will consider retail (sales suppression) frauds, notably those facilitated by technology, and the importance of securing transaction data at the point of sale and then storing it centrally (Croatia), or having immediate central access to it at the retail location (Rwanda).

[10] NF-e is the acronym for *Nota Fiscal Eletrônica.*

[11] CT-e is the acronym for *Conhecimento de Transporte Eletrônico de Cargas*.

[12] For a further (and an extreme) example – within the same legal entity, moving goods between two branches, inside the same city, using their own trucks (so there is no need for a CT-e), the company will still need to issue a NF-e for the transfer (there is an output debit for the dispatching branch - accounting is made by branch - and an input credit for the receiving branch). [Example provided by Camilo Martinez, a Brazilian tax attorney with Thomsonreuters specializing in transaction taxes.]

SPED in Brazil

SPED's adoption required a constitutional amendment because tax information was to be shared among state and federal governments. This was accomplished in 2003.[13] A Third Invoicing Directive, one that follows the suggestions in this paper may raise similar concerns about tax information sharing in the EU. A regulation may be necessary.[14]

How NF-e and CT-e operate. The NF-e and CT-e function in a very similar manner. The major difference between them is that the immediate object of the NF-e are the goods sold across internal borders. The immediate objects of the CT-e are the commercial services that transport the goods. As time progressed this cross-border system has become part of the basic internal tax system. An example helps:

Assume firm "A" (in state 1) sells goods to firm "B" (in state 2), and also assume that the goods will be transported by a common carrier hired by firm "A."

STEP 1: Firm "A" will generate two electronic files in XML format[15] (one for the NF-e; the other for the CT-e) that will contain all necessary tax information for the sale of goods and the sale of transport services (in other words, a digital invoice).[16]

- The issuer digitally signs the files (to assure integrity of the data and authorship);[17]
- The files are transmitted (through the Internet) to the State tax administration in State 1; and
- The transmission constitutes a "request for authorization" to use a NF-e, or CT-e.[18]

STEP 2: The State Tax Administration in State 1 (the origin state) acts on the authorization of use request, without which there can be no binding contract for the

[13] Constitutional Amendment No. 42 of December 19, 2003 (See: *Constitution of the Federal Republic of Brazil* of October 5, 1988, Art. 37).

[14] Article 288, para. 2, TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION.

> A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.

Consolidated text *available at*: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0047:0199:en:PDF

[15] XML is an acronym for eXtensible Markup Language. It is a set of rules for encoding documents in machine-readable form. It is defined in the XML 1.0 Specification produced by the World-Wide Web Consortium (W3C), and several other related specifications. These are gratis open standards.

[16] It is important to note that these are not "heavy" files. For example, a large supermarket with gross revenues of US$ 1 billion per year, and millions of invoices, would probably deliver a 5 megabyte file in a month. [Example provided by Brazilian tax attorney Eric Kanno, currently an LLM candidate at Boston University School of Law.]

[17] The digital certificate in Brazil is provided by Certsign at: http://www.certisign.com.br/ and Serasa at: http://serasa.certificadodigital.com.br/

[18] The transmission to the State Tax Administration is for *Impostos Sobre Circulação de Mercadorias e Prestação de Serviços* (ICMS) verification. The ICMS is the state sales tax and the rate varies depending upon the industry and the Sate.

provision of goods, and no supply of services under commercial law. Authorization is not difficult.

- The authorization system is fully automated (without human intervention);
- Authorization is available 24/7;
- The authorization process is a basic check of the XML file for accuracy and completeness;
- Although a period of up to 3 minutes is allowed for the authorization process, in reality authorization takes a few seconds, and commonly takes only a millisecond.

STEP 3: If the XML file is accurate, the State Tax Administration in State 1 responds in two ways:

- It returns to the Seller an Authorization of Use notice; and
- It transmits the NF-e to the Treasury Department of the Federal Revenue Service (it is placed in a national depository of all NF-e's issued in the country).[19]

STEP 4: Firm "A" produces a simplified picture of the NF-e on plane paper to accompany the transit of the goods:

- The document is called DANFE (*Documento Auxiliar da Nota Fiscal Eletrônica*, or Electronic Invoice Auxiliary Document);[20]
- DANFE contains an access key with which the official NF-e can be accessed over the Internet for verification of complete invoice data appearing on the DANFE;
    - The access key is primarily a fixed-size alpha-numeric bit string;
    - The access key is also reproduced on the DANFE as a bar code in Code 128-C format;[21]
- The bar code is intended to facilitate verification of the NF-e at inspection stations on the internal Brazilian borders (but it also functions in an audit context to immediately call up - in real-time - any invoice in the Brazilian commercial system with the press of a button).

STEP 5: With the printed DANFE and authorization of the NF-e the shipment of the goods can begin.

STEP 6: The Seller will deliver (make available to) the buyer in State 2 the following:

- NF-e (as a digital file) [and/or CT-e];
- Authorization of Use (as a digital file) [for both NF-e and/or CT-e] either

[19] The transmission to the Federal Revenue Service is for verification of tax status with respect to three federal levies: (1) the *Imposto sobre Produtos Industrializados* (IPI); (2) the *Programa de Integração Social* (PIS); (3) the *Contribuição para o Financiamento da Seguridade Social* (Cofins). The IPI is a non-cumulative federal tax on industrial goods. PIS is a social contribution tax payable by corporations to finance the payment of unemployment insurance. Cofins is a federal tax based on gross revenues of business sales.

[20] The same process is duplicated for transportation services. The only significant differences are: (1) instead of a NF-e the primary document is a CT-e; and (2) instead of a DANFE the paper reproduction is called a DACTE (*Documento Auxiliar do Conhecimento de Transporte*, or the Auxiliary Document of Electronic Waybill).

[21] Code 128 is a very high-density barcode symbol. It is used for alphanumeric or numeric-only barcodes. It can encode all 128 characters of ASCII. There are three types of Code 128, the A, B, and C versions. Brazil uses the "C" subtype.

- DANFE (plane paper copy of the NF-e with internet access key) [or DACTE]

STEP 7: When goods are delivered to the Buyer, the Buyer will:

- Go to the web site of the Treasury Department of the Federal Revenue Service and use the access keys[22] to:
    - Check the validity of the DANFE;
    - Check the validity of the DACTE.

Brazilian cross-border tax fraud
"invoice sightseeing"

SPED, NF-e, and CT-e are not primarily directed at tax fraud, they are part of a larger move to e-documentation in commercial affairs. However, these particular documents are coordinated by the tax administrations and they do verify the tax on cross-border B2B transactions. The tax must be calculated and stated on the invoice in order for it to be considered complete.

These documents have almost eliminated one of the most difficult Brazilian cross-border tax frauds to deal with – "invoice sightseeing," or *nota fiscal fria* ("cold invoice"). Oldman and Schenk explain how the fraud operates:

> For example, assume that the rate in state A on domestic sales is 17 percent and on interstate sales to state B is 7 percent. A seller in state A sells goods to a "buyer" (a wholesaler) in state B. The wholesaler in state B then resells the goods to a small business back in state A and applies the interstate rate of 7 percent. [However,] only invoices are exchanged, the goods in fact are shipped from the seller in state A to the small business in state A, and the small business in state A saves 10 percent tax. This is tax advantageous if the small business is exempt … and cannot recover tax on purchases.[23]

In this example if the seller in state A had secured a NF-e and CT-e from the tax administration in state A (as he is required to do to have a binding contract under Brazilian commercial law), and if the goods never crossed the border to state B, and if the buyer never acknowledged receipt of the goods in state B, the outcome is clear. **There will be an audit. The system demands it.**

The old fraud would not even begin if a commercial carrier were involved. No commercial carrier in Brazil today will pick up goods without a CT-e (or the DACTE).

When de Mello, Dias, Fontana and Fernandez assess the effectiveness of Brazil's electronic tax documents against intra-state tax fraud they underscore that it is the *real-time control* that this system gives over commercial information flows that is the key to its success.

> On the side of the Tax Authorities, NF-e [and CT-e] represents an

[22] The access keys are available in alpha-numeric and bar code format on the DANFE and DACTE, but are also contained in the NF-e and CT-e electronic files.

[23] Alan Schenk & Oliver Oldman, VALUE ADDED TAX – A COMPARATIVE APPROACH 383 at n. 75.

> important tool to fight against tax evasion, as *it permits control, in real time, of the information on the commercial transactions* performed by the companies and as it permits the integrated work between the Federal and State Tax Authorities, upon the interchange of information.
>
> These electronic documents have common information and CT-e has fields that may refer to NF-e, … [the text goes on to list a large number of common data fields].[24]

SPED v. VIES

SPED and VIES are companion data-sharing regimes. Both endeavor to prevent a kind of tax fraud that exploits inter-jurisdictional information gaps. Both "invoice sightseeing" and MTIC frauds work in the same way. They capture all or some of the tax paid on an onward sale of a cross-border supply that previously benefited (perhaps improperly) from a reduced rate of tax.

"Invoice sightseeing" and MTIC both involve pre-arranged transactions among conspiring taxpayers. In both cases stopping the fraud requires the tax authority to receive accurate and timely information about the nature of the fraudulent transactions. This information needs to be available in *real-time*. Immediacy, more than any other factor, explains why SPED is more effective than VIES. SPED shares critical tax data in real-time; VIES delays data sharing for six months or longer.[25]

[24] Newton Oller de Mello, et. al., *The Implementation* at *supra* note 6, at 454 (emphasis added).

[25] It was not uncommon for the data underlying a 1993 VIES inquiry to be six months old (or more) by the time it got to the tax inspector who needed it. The VIES relied on quarterly recapitulative statements [VAT Directive, Article 22(6)(b) and Council Regulation 218/92, Article 4(1)], and jurisdictions responding to VIES requests were allowed an additional three months to reply [Council Regulation 218/92, Article 4(4)].

When one realizes that a full MTIC cycle can be completed in an afternoon and the money from the fraud can be on deposit within thirty days, it is not surprising that the 1993 VIES was not very effective in the fight against missing traders.

Fraudsters can disappear long before the tax authority secures the records of suspect transactions. At the height of the UK MTIC fraud in computer chips the *Guardian* newspaper interviewed a fraudster.

> [MTIC fraud] is Britain's fastest-growing criminal enterprise, ... Among the [criminals is] a man who likes to be known as Colin, a genial wheeler dealer, ... and his mate "Andy", said to be "a bit of an anorak" when it comes to computers. "He's the technical expert," Colin explained. "I'm into banking, investments, things like that." Each afternoon, hunched over a couple of PCs in his apartment ... Andy spins the wheels of carousel fraud, ... "You can turn the carousel in just 10 minutes, and then you just have to wait 30 days for the money to come in," says Colin. "You can run it round five companies but there are up to 300 that can be used. Each spin can give you up to 200,000 pounds. The longest it stays in any bank account is two hours. ... You can move money so fast. The scale of it is beyond comprehension, you have no idea how much money is being made." ... The downside, as Colin and Andy discovered late last year, is that carousel fraud is becoming increasingly attractive to violent criminals. ... "Andy had a knock on his door [one day] and then he found he was having to pay out to some really heavy people ... I thought he was going to get cracked. He didn't get cracked, but, ..." [said Colin].

Ashley Seager & Ian Cobain, *Carousel fraud: Bogus deals keep Customs in a spin: Smart criminals stay ahead of investigators Russian mafia and IRA linked to swindles,* GUARDIAN (May 9, 2006) *available at*: http://www.guardian.co.uk/uk/2006/may/09/ukcrime.ashleyseager

VIES is older than SPED. VIES developed out of an income tax model of information sharing. The guiding principal under this model is that a jurisdiction should *request* the information that it needs, and the *request* should be rooted in an investigation.

The VIES expanded as the EU did. In 1993 there were twelve Member States.[26] These twelve became fifteen in 1995,[27] then twenty-five in 2004,[28] and twenty-seven by 2007.[29] Even with this growth, the VIES remained largely unchanged from its income tax information sharing roots. The VIES is (primarily) a request-based, sales-side-only information exchange. It is digitally handicapped largely because it uses technology to replicate, rather than revise and replace, its traditional approach to information sharing.

Some have blamed the relentless expansion of the EU for its failure to adopt more technology-intensive solutions to MTIC through the VIES. In some states (so the argument goes) technology could overburden the domestic infrastructure.[30] This has not been Brazil's experience. SPED produces real-time, invoice-level, matched purchase/sales, cross-border controls with simple XML files.

The core reason for the difference between the VIES and SPED is that SPED is based in a fundamentally different data-sharing model. Under this model tax data can be gathered and shared broadly. It can be shared based on a *general not a specific need.* It is secure, and access is limited to government officials who have a need for it. It is real-time commercial data and should be protected, but it is not personally identifiable information (PII). As a result, SPED does not wait for a formal request to share information – it is there when needed and often before the tax is due.

The EU clearly has something to learn. A brief review of the VIES is warranted.

VIES in the EU

The VIES developed in three stages: the initial goods-based phase (1993 through 2003); the consolidation phase (2003 through 2010); and the expansion into services phase (2010 through the present).[31]

[26] The twelve are: Belgium, Denmark, France, Germany, Greece, Ireland, Italy, Luxembourg, the NETHERLANDS, Spain, the United Kingdom and Portugal.

[27] Austria, Finland and Sweden joined the EU.

[28] The ten additions are: Cyprus, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovenia, and Slovakia.

[29] Bulgaria and Romania joined the EU.

[30] Radu Lixandroiu, *An Analysis of Combating VAT Fraud in the European Union Using New IT Technologies,* 2 BULL. OF THE TRANSYLVANIA, U. OF BRASOV 105, 107 (2009) (referencing a Romanian study indicating that only 81.9% of Romanian organizations have computers; 64.16% use the internet; 27.97% of Romanian organizations have websites; and only 7.15% use online shopping).

[31] It is important to note that this "development" was neither intended nor anticipated. The VIES was set up as a very short-term solution to what was perceived to be a potential problem area. MTIC was anticipated. No one at the time imagined that the VIES would still be in operation twenty-years later.

> When the VIES was set up in 1993, it was built to last four years, the time the transitional VAT arrangements were initially expected to last. However, it has now been running for much longer. Though the system has been successful in providing control information on the bulk of intra-community trade, its shortcomings are more and more apparent.

The initial phase (1993-2003). The first EU rules on exchanges of VAT information predate the VIES by fourteen years. A 1979 Directive[32] simply extended the Directive on mutual assistance in direct taxation into VAT. It allowed simple government-to-government sharing of VAT information.[33] The VIES never wanders far from this income tax information-sharing model.

Limited automation came to the VIES later. A 1992 regulation that became effective the following year (coincident with removing the internal customs borders on January 1, 1993) brought technology to the VIES.[34]

The 1993 VIES allowed businesses selling goods into other Member States to quickly determine the validity of their customer's VAT registration, thereby supporting the zero-rating of the supply.[35] The VIES also stored in its network of country-by-country databases an aggregate record of all intra-EU taxable goods transactions. Thus, the VIES could be marshaled to assist government auditors. It allowed matching of VIES (sales) data with purchases data reported on returns. Authorities could also perform risk assessments with the VIES, trying to identify traders who might go missing.[36]

VIES data comes from the recapitulative statements filed by registered taxpayers that make cross-border sales of goods. Services were added to the VIES in 2010. Two sets of records are provided:

- VAT identification numbers of cross-border sellers and buyers, and
- The total value of all intra-Community supplies of goods made (during the reporting period) by a specific seller to an identified buyer.

However, VIES data is neither collected, nor distributed in real-time. It is not invoice-specific, nor is it granular, or presented transaction-by-transaction. VIES data is delayed and aggregate.

Even though the VIES is computerized,[37] it does not maintain a match-able cross-border transactional database.[38] Essentially, the VIES functions as a forwarding service. It forwards inquiries made by one Member State to other Member States. When

Report from the Commission to the Council and the European Parliament on the use of administrative cooperation arrangements in the fight against VAT fraud (COM 260) 9 (2006).

[32] Council Directive 79/1070 amending Directive 77/799/EEC concerning mutual assistance by the competent authorities of the Member States in the field of direct taxation O.J. (L 331) 8-9 (1979).

[33] Council Directive 77/799 concerning mutual assistance by the competent authorities of the Member States in the field of direct taxation, O.J. (L 336) 15-20 (1977).

[34] Council Regulation 218/92 of 27 January 1992 on administrative cooperation in the field of indirect taxation (VAT) O.J. (L 024) 1-5 (1992).

[35] VIES provides a real-time answer to anyone seeking to verify an EU VAT registration number for a specific firm in a specific country. See: http://ec.europa.eu/taxation_customs/vies/vieshome.do?selectedLanguage=en

[36] Donato Raponi, *International Exchange of VAT information within the EU*, (powerpoint) slide 3 of 22 (the Head of the Unit for Administrative Cooperation and Fight against Tax Fraud, European Commission in a presentation on the history of the VIES in the EU).

[37] Council Regulation 218/92, *supra* note 34.

[38] Radu Lixandroiu, *supra* note, 30 at 107.

responses come back from the independently maintained database of the other Member State, the VIES re-forwards these answers to the inquiring party.[39]

The VIES allows three types of exchanges: (1) *assistance on request*[40] (where the initiative lies with the applicant); (2) *automatic assistance*[41] (where both the applicant and the requesting party have agreed in advance that certain types of information will be collected and exchanged automatically); and (3) *spontaneous assistance*[42] (where one party takes the initiative to make an exchange without being requested to do so).[43] The vast majority of uses fall into category (1).

The consolidation phase (2003-2010). MTIC fraud reached epidemic proportions by mid-2000. Even though the VIES was designed to deal with exactly this kind of fraud, it could not contain it.[44] In the 2000 Report to the Council and European Parliament the Commission indicated that the VIES failed because the States were not using it, and the States were not using it because the VIES was slow and cumbersome.

In 2001 the Commission found that Member States were "… unwilling (or unable) to provide details of additional tax discovered as a result of the information exchanged over the VIES."[45] It found that MTIC fraud was accelerating, but "…

[39] Council Regulation 218/92, *supra* note 34, at art. 4(1) (requiring the competent authority of each Member State to maintain an electronic database).

[40] *Id*., at art. 5(1) (indicating further in Article 5(2) that additional information can include invoice numbers, dates, and values in relation to individual transactions, and also in Article 6(3) the name and address of the person to whom a VAT identification number is issued).

[41] *Id*., at art. 4(2).

[42] *Id*., at art. 12.

[43] Commission, Proposal for a Council Regulation (EEC) concerning administrative cooperation in the field of indirect taxation, COM(183) 7 (1990).

[44] Great Britain: Parliament: House of Lords: European Union Committee, Stopping the Carousel: Missing Trader Fraud in the EU – Report with Evidence, 12-13 (2007).

> In the UK, levels of MTIC fraud have risen since it was first identified and measured in the late 1990s. However, like any criminal activity its nature makes it difficult to measure, and we have been presented with a variety of different estimates of the size of the activity. HMRC's estimates are contained in table 1:

Year	Estimated size of MTIC fraud – HMRC
1999/2000	£1.5 – £2.4bn
2000/01	£1.3 – £2.5bn
2001/02	£1.7 – £2.5bn
2002/03	£1.5 – £2.3bn
2003/04	£1.1 – £1.7bn
2004/05	£1.1 – £1.9bn
2005/06	£3.5 – £4.75bn

Jasper Copping & William Langley, *The £30 billion money-go-round*, The Telegraph (August 20, 2006), (indicating that the UK-Dubai export/import trade was apparently very lucrative in the mid-2000s, until it was realized that this was a favored MTIC route for traders. "The total loss since the mid-1990s, when the fraud first emerged, is estimated to be as much as £30 billion.")

[45] Report from the Commission to the Council and the European Parliament, Third Article 14 Report on the Application of Council Regulation (EEC) No. 218/92 of 27 January 1992 on Administrative Cooperation in

Member States' use of the [VIES] … had not increased significantly … "[46] MTIC was now driving the VIES to change if it was to stay relevant to MTIC investigations.[47]

More changes came in 2003. Council Regulation (EC) No. 1798/2003 replaced Regulation (EEC) No. 218/92. Legal provisions were unified and critical elements of the 1977 Mutual Assistance Directive were directly assimilated.[48] The express intent was to make the VIES a more effective weapon against MTIC.

> (1) *a single legal basis was established for all information requests* – where previously a request needed specify invoice numbers, dates and values of specific transactions, now a comprehensive request for information could be made;[49]
> (2) *simultaneous controls* – a new structural framework for multilateral control was established, replacing bilateral controls;[50]
> (3) *intensified exchange of relevant information* – the new regulation provided a structure for broad-based intra-Community information sharing;[51]
> (4) *legal grounding and a mechanisms to facilitate third country information sharing and exchange* – information exchange could now include all Member States and third countries;[52] and

the Field of Indirect Taxation (VAT) and Fourth Report Under Article 12 of Regulation (EEC, Eurotom) No. 1553/89 on VAT Collection and Control Procedures COM(28) 23 (2000) at 21.

[46] *Id*.

[47] Commission, Proposal for a Regulation of the European Parliament and of the Council on administrative cooperation in the field of value added tax & Proposal for a Directive of the European Parliament and of the Council amending Council Directive 77/779/EEC concerning mutual assistance by the competent authorities of the Member States in the field of direct and indirect taxation COM(294) 2-3 (2001) (emphasis added):

> In the opinion of the officials responsible for controls in the Member States and the Commission, the VIES system and the strengthened administrative cooperation introduced by Regulation (EEC) No 218/92 are effective instruments of control.
>
> However, the information exchanged automatically or on request from the recapitulative statements provided by taxable persons is *not available early enough* and cannot be exchanged as quickly as needed, so does not help in fighting fraud effectively. Post-clearance checks are often too late and the provisions of Regulation (EEC) No 218/92 were never intended to deal with individual cases of fraud, which by their nature are immediate. Moreover, the scope of the Regulation does not cover all the transactions that could give rise to fraud. It relates only to intra-Community supplies and acquisitions and not, for instance, to domestic supplies or *services*. Since most VAT-fraud schemes concern both intra-Community and domestic transactions, the tax authorities are obliged to make use of other legal instruments.

[48] O.J. (L 264) 1 (2003).

[49] *Id*., at art. 5.

[50] *Id.,* at arts. 12-13. Because MTIC is a cross-border fraud the use of multilateral controls (coordinated controls of the tax situation of one or more taxable persons with common interests in multiple jurisdictions) is central to the enforcement effort. However, these kinds of controls were falling in use.

> The Commission cannot but be alarmed at the fall in the number of such controls, which was already low, despite their being financed by the budget of the *Fiscalis* program. Only three controls were organized in the whole European Union in 2003, four in 2002 and eight in 2001 (compared with 15 in 2000, a figure which was already low when set against the 1,500,000 businesses engaged in intra-Community transactions).

Report from the Commission to the Council and the European Parliament on the use of administrative cooperation arrangements in the fight against VAT fraud, COM(260) 12 (2004).

[51] O.J. (L 264) 1 (2003) at arts. 17-21.

(5) *digital exchange* – exchanges were to be made by electronic means.[53]

The VIES was still slow, and still request-based. Regulation 1798/2003 did very little to expedite access to information. A six-month or longer wait remained the norm.[54] In addition, nothing was done to deal with MTEC in cross-border services, even though by 2003 MTIC was morphing into *services-based* frauds. Service frauds were penetrating the VoIP market,[55] and destroying the market for CO2 permits.[56] The VIES was simply not able to handle MTIC as it developed.[57]

The Expansion into services phase (2010-present). A third set of VIES revisions came in 2008, effective January 1, 2010.[58] Council Directive 2008/8/EC added language to Article 262 of the VAT Directive that included *services* in recapitulative statements.[59]

[52] *Id.*, at art. 36.

[53] *Id.*, at art. 37.

[54] *Id.*, at arts. 8 & 25. However in paragraph 2 of Article 8 an exception applies where "the requested authority is already in possession of that information, the time limit shall be reduced to a maximum period of one month."

[55] *Phuncards-broker* was a VoIP MTIC fraud embedded in a global money-laundering scheme that involved Telecom Italia SpA and FastWeb SpA. During 2003 and then 2005 through 2007, this fraud (allegedly) cost Italian taxpayers €400 million. See: Richard T. Ainsworth, *The Italian Job – Voice Over Internet Protocol MTIC Fraud in Italy*, 58 TAX NOTES INT'L 721 (May 31, 2010).

[56] Trade in greenhouse gas emissions was to commence on January 1, 2005. [DIRECTIVE 2003/87/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a scheme for greenhouse gas emission allowance trading within the Community and amending COUNCIL DIRECTIVE 96/61/EC, O.J. (L 275) 32 (October 13, 2003)]. The VAT Committee met and determined that CO2 certificates were to be treated as a service on May 27, 2004. [VALUE ADDED TAX COMMITTEE, WORKING PAPER 443 REV 1, *Question Concerning the Application of Community VAT Provisions: Greenhouse Gas Emission Allowances*, TAXUD/1625/04 REV 1 (May 27 2004) & European Commission, Taxation and Customs Union, *A Selection of Guidelines Adopted by the VAT Committee from 1977 to 2008* (as of December 31, 2008) with regard to QUESTIONS concerning the application of the Community VAT provisions.]

[57] CO2 MTIC/MTEC is the 2003 VIES' perfect storm. Not only are CO2 certificates deemed to be *services* (and outside the scope of recapitulative statements) but CO2 MTIC/MTEC takes *less than 15 minutes* to complete on the BlueNext Exchange. An individual at a Parisian café needs only a laptop to be an effective CO2 fraudster. See generally: Richard T. Ainsworth, *CO2 MTIC Fraud – Technologically Exploiting the EU VAT (Again)* 57 TAX NOTES INT'L 357, 358 (January 25, 2010).

[58] The "VAT Package" is a series of measures that change the VAT rules relating to services. It introduces a Directive on the place of supply of services, and a new VIES-based reporting obligation for cross-border services (a Regulation), a mini one-stop-shop for telecom, broadcasting and e-commerce, and a Directive that announcing a new process for recovering VAT through existing international refund mechanisms. Agreement on the VAT Package was reached on December 4, 2007, although the provisions within it were not effective until January 1, 2010. Europa Press Release, *VAT Package: Commission welcomes adoption by the ECOFIN Council of new rules on the place of supply of services and a new procedure for VAT refunds*, IP/08/208 (December 2, 2008) *available at*: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/208

[59] Council Directive 2008/8/EC at Article 2(9) changing Article 262 of Directive 2006/112/EC. O.J. (L 44) 11 at 16 (February 20, 2008). Article 262(c) reads:

> Every taxable person identified for VAT purposes shall submit a recapitulative statement of the following …
>
> (c) the taxable persons, and the non-taxable legal persons identified for VAT purposes, to whom he has supplied services, other than services that are exempted from VAT in the Member State where the transaction is taxable, and for which the recipient is liable to pay the tax pursuant to Article 196.

Information exchange was accelerated. Council Directive 2008/117/EC required monthly recapitulative statements, except for:

- Taxpayers who supply less than 100,000 euro in goods in a quarter,[60] until December 31, 2011 when the ceiling fell to 50,000 euro;[61] and
- All service providers, who remain on quarterly statements.[62]

The data collected from recapitulative statements remained relatively high-level. It was not the invoice-specific, granular data of the SPED. The VIES collects the following six types of data:[63]

- The VAT identification number of the taxable person submitting the recapitulative statement, and who has made a zero-rated supply under Article 138(1) for goods, and under which he has made a taxable supply of services under Article 44.
- The VAT identification number of the person acquiring the goods or services.
- The VAT identification number of the taxable person who must submit a recapitulative statement under Article 138(2)(c) [triangulations], and the number by which he is identified where the dispatch or transportation ended.
- The total value of goods, and total value of services per recipient.
- The total value of goods transferred per recipient under Article 138(2)(c) [triangulation].
- All adjustments made pursuant to Article 90 [cancellations, refusals, total or partial non-payment].

Proposal -
A Third Invoicing Directive/Regulation

In terms of stopping cross-border frauds, the Brazilian SPED works. The EU VIES does not. Brazil's system works because it is *invoice-based*, not *report-based.* SPED is a digital, real-time, invoice solution that uses light data files. The VIES is a summary, report-based solution that uses aggregate data that is several months old.

The major *system* difference between the SPED and this proposal is in the role of Brazil's Treasury Department of the Federal Revenue Service. This function is replicated digitally on the VAT invoice, not structurally. It is assumed that Member States would object to having a central authority in Brussels hold all domestic invoice data, but that they would not object to providing access to data from discrete cross-border transactions that involved their taxpayer and its commercial companion in another Member State.

[60] Council Directive 2008/117/EC at Article 1(3) adding Article 263(1b) to Directive 2006/112/EC, O.J. (L 44) 11.

[61] Council Directive 2008/117/EC at Article 1(3) adding Article 263(1a) to Directive 2006/112/EC. O.J. (L 44) 11, at 8 (January 20, 2009)

[62] Council Directive 2008/117/EC at Article 1(3) adding Article 263(1c) to Directive 2006/112/EC, O.J. (L 44) 11.

[63] The VAT Directive, Council Directive 2006/112/EC of 26 November 2006 on the common system of value added tax, art. 264, 2006 O.J. (L 347) 1.

There are nine steps in this proposal. They specify the *method* that must be followed and requires that *two digital signatures* be added to every VAT invoice.

STEP 1: Each Member State is required to dedicate a secure digital storage facility with sufficient capacity to store electronic invoices for the entire domestic economy.

STEP 2: Each seller will generate an electronic file in XML format containing all data needed for an invoice.

- The issuer will digitally sign the file (to assure the integrity of the data and its authorship);[64]
- The file will be transmitted (through the Internet) to the Member State 1 database; and
- The transmission will constitute a "request for authorization" to issue an intra-community invoice that would support:
  - a zero-rated supply of goods under Article 138(1),
  - a taxable supply of services under Article 44, or
  - a zero-rated triangular supply under Article 138(2)(c).

STEP 3: The Tax Administration in State 1 (origin) will act on the Authorization request.

- The authorization system will be fully automated (without human intervention);
- Authorization will be available 24/7;
- The authorization process is a basic check of the XML file for accuracy, completeness, and an automated risk assessment (an comprehensive risk assessment may be completed without delaying the authorization process if necessary);
- Authorization and risk assessment should be expected in less than three minutes (as under the Brazilian model). In reality it should take a few seconds or milliseconds. The standard should be: a time that is not longer than the credit card approval for retail transactions.

STEP 4: After assessment the Tax Administration in State 1 (origin) will save the XML file, and if the XML is approved the Tax Authority will respond in two ways:

- It will return to the Seller an Authorization message which will:
  - Contain an access key that will allow access to the digital invoice over the Internet. The access key:
    - Will be a fixed-size alpha-numeric bit string;
    - Will also be a reproducible bar code in Code 128-C format
- It will transmit the access key to the Tax administration in State 2 (destination).

STEP 5: The Seller will transmit this data (with the access key embedded in the digital file, or with the bar code reproduced on a paper invoice) to the Buyer.

[64] For example this kind of certification is provided in the Croatian system by FINA at: http://www.fina.hr/Default.aspx

STEP 6: The Buyer will generate an electronic file in XML format replicating the file received in STEP 5 (with embedded access key) and transmit the file through the Internet to the Tax Authority in State 2 (destination). This transmission:

- Will be digitally signed by the Buyer;
- Constitutes a "Request to Proceed with an Intra-Community Acquisition;"
- Notify the Tax Administration in State 2 that the Buyer plans to reverse charge this acquisition.

STEP 7: The Tax Administration in State 2 (destination) will save the file and perform an "Authorization and Risk Assessment procedure." An approval has three results:

- An Authorization message is sent to the Buyer;
- The message will include a second digital access key (like that in STEP 4) allowing Internet-based verification of the data submitted in STEP 6.
- A copy of the second access key is sent to the Tax Administration of State 1.

STEP 8: The Buyer will return to the Seller a final XML data file containing:

- The essential data elements of the invoice;
- The access code from State 1; and
- The access code from State 2.

STEP 9: The Seller will now issue the *VAT Invoice* to the Buyer. The VAT Invoice must contain both access codes.

Preventing MTIC With the Third Invoicing Directive

This proposal for a Third Invoicing Directive will stop the vast majority of MTIC frauds. Unfortunately, the proposal is not perfect. There is a small window for MTIC/MTEC frauds that remains open. That window is the space between an intra-community acquisition (or other zero-rated purchase) and the due date of the return where the reverse charge should appear. MTIC/MTEC can still occur here.

This gap needs to be closed with effective audit. One of the additional strengths of this proposal is that it places within each Member State's domestic database all the transactional data of the taxpayers within its jurisdiction. Closing the gap may not be overly difficult, and tax losses arising in the gap can in many instances be retroactively neutralized (because returns have not been filed). Enforcement can be in real-time.

Examples are helpful. The first is a simple two-party example; the second uses buffer companies.

Example 1

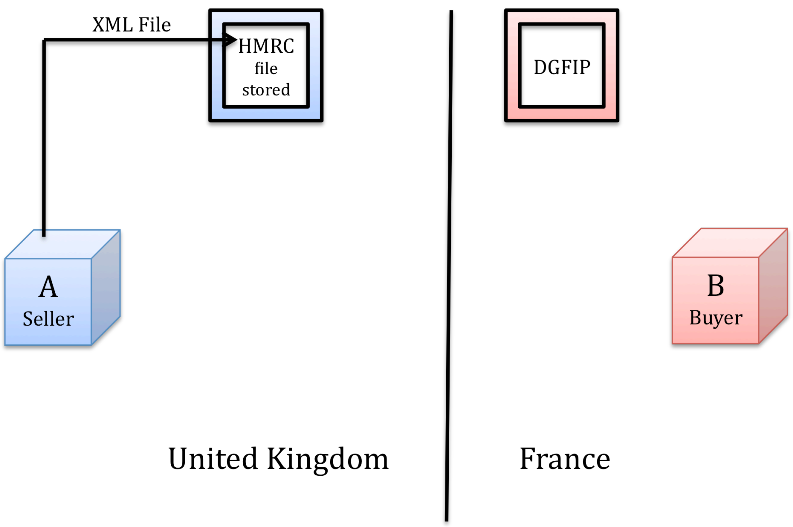
Assume that Firm "A" in the UK agrees to sell a specific quantity of identified high-value goods to firm "B" in France. The price is set. The time and method of delivery are also agreed. Firm "A" plans to zero-rate the sale and recover the input VAT it paid on purchases. Firm "B" is expected to perform a reverse charge in France.

MTIC fraud would arise if Firm "B" did not perform the reverse charge, did not file a return, and sold the goods on to Firm "C" in France and collected VAT on the new selling price.

Under the proposal, after reaching an agreement for the sale Firm "A" sends an XML file to the UK tax authorities (Her Majesty's Revenue and Customs [HMRC]). The file will contain all required information for an invoice, and be digitally signed to assure data integrity and authorship. This file is essentially a pro-forma invoice.

HMRC will check the data for completeness, and run a risk assessment program against it. HMRC will look for things like a past history of fraud, or unusually large volumes, exceptionally large payments, or indications that payments are to be made to off shore third parties. Risk factors will be locally determined, but might also include factors like whether or not seller or buyer was newly registered. This transmission to HMRC is an advance notice that this taxpayer will claim a VAT refund in the near future. *See*: Figure 1.

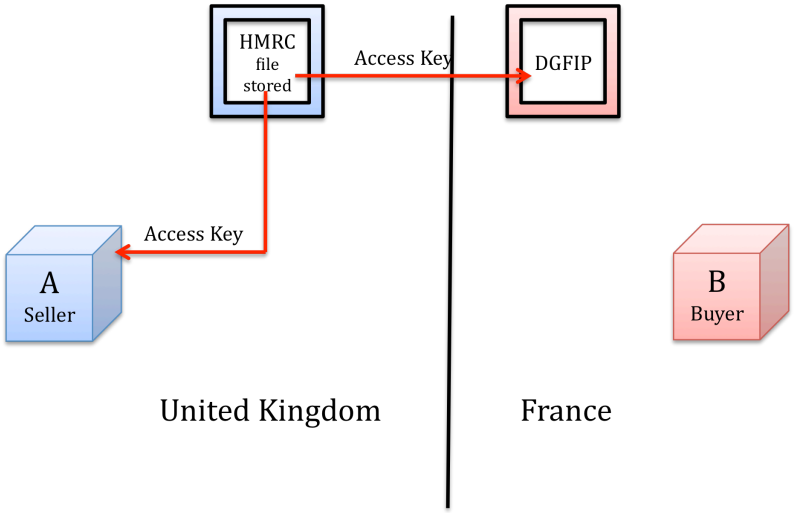
Figure 1



The XML file will be saved by HMRC, and an Internet access key to it will be produced. If the outcome of the authorization process is satisfactory, the key will be transmitted to Firm A.

The same access key (along with notification of authorization) is simultaneously sent to the French tax authorities (Direction générale des finances publiques [DGFIP]). This advance notice of a potential French supply will allow DGFIP to perform a companion risk assessment. *See*: Figure 2.

Figure 2



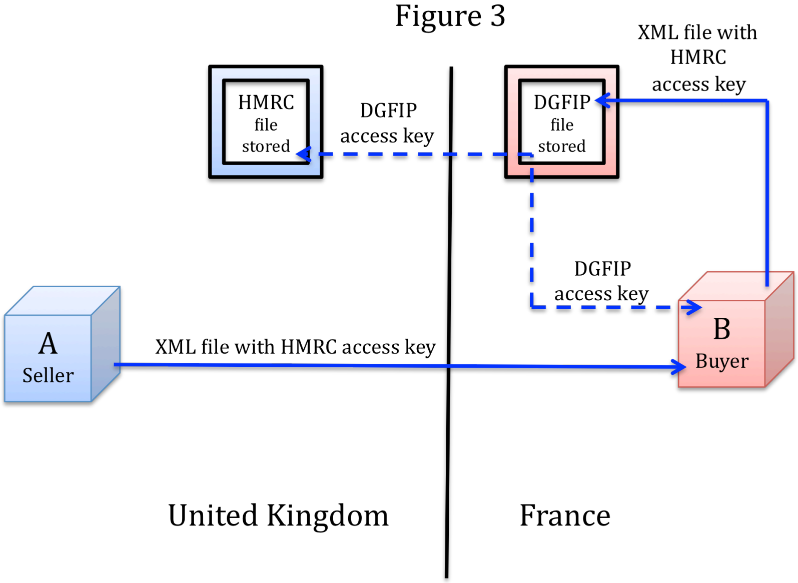
With the access key in hand Firm "A" will transmit the XML file and access key to Firm B. Firm "B" will replicate the XML file and send it to DGFIP. This file will be digitally signed by Firm "B" to assure data integrity and authorship. This transmission is a request for authorization to proceed.

DGFIP will save a copy of the XML file, match this file against the file received from HMRC (via the access key sent by HMRC), and then run a risk assessment tool against the proposed transaction. If no problems are detected DGFIP will generate a second access key (through which the XML file saved by DGFIP can be pulled up) and send it to both Firm "B" and HMRC.

DGFIP's concern is whether or not Firm "B" is likely to become a missing trader. If Firm "B" does not perform a reverse charge, does not file a French return, and sells-on the goods it purchased from Firm "A" (charging VAT), then there will be an immediate tax loss in France. It will be difficult to know this for sure prior to the due date of the French return. As a result, DGFIP's automated risk assessment program should be fine-tuned.

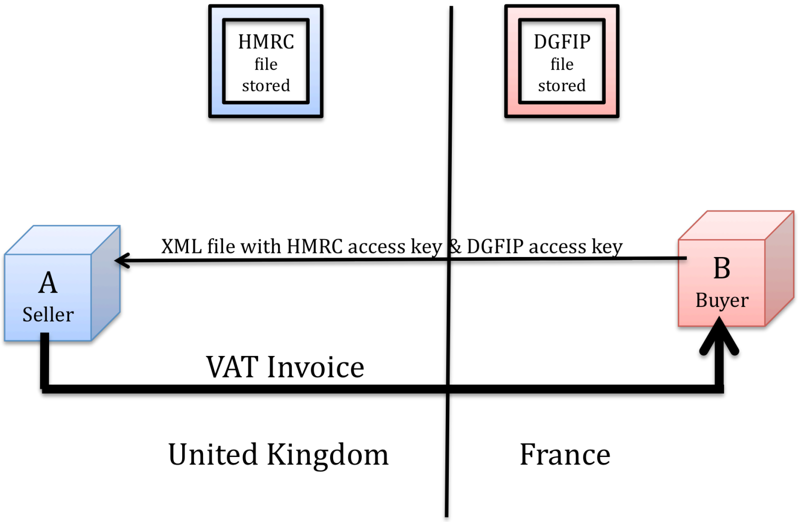
The proposal provides the DGFIP with two opportunities to anticipate a missing trader fraud. If no problem is foreseen, but fraud arises anyway, then the scope of the fraud will be limited to the period before the next return is due. If DGFIP knows a return is due and if no return is filed, then any further transactions involving Firm "B" will fail risk assessment. See: Figure 3.

Figure 3



The final step in the proposal requires Firm "B" to return the XML file to Firm "A" with both access keys embedded in the data. Receipt of this file from Firm "B" is the final step before Firm "A" drafts the VAT invoice. See: Figure 4.

Figure 4

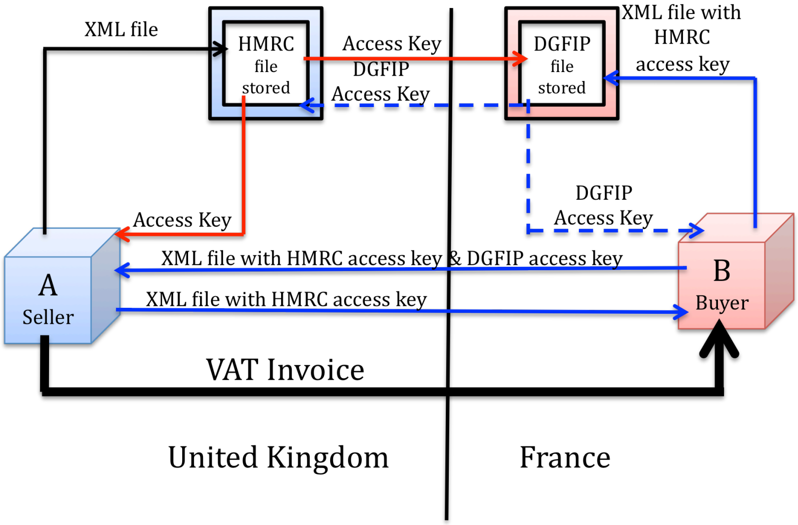


This proposal allows HMRC and DGFIP to match purchases and sales in real time. The matching occurs in advance of the transactions, and when returns are filed additional matches can be performed. In other words, HMRC will be able to conduct a preliminary audit of Firm "A's" claim for zero-rated intra-community supply to Firm "B" by digitally matching from *within its own database*:

- Draft invoices, the
- VAT invoice, and the
- VAT returns.

In a similar fashion DGFIP will be able to conduct a preliminary audit of Firm "B's" reverse charge on its intra-community acquisitions from Firm "A." See: Summary Figures 1-4.

Summary Figures 1-4



Audits conducted with the assistance of the VIES are far more limited. The VIES will only allow DGFIP to compare the reported sales by Firm "A" (in aggregate) with Firm "B's" return position. This comparison can be made (roughly) six months after the suspect transactions are completed. As such, the VIES has almost no preventive value, and to the extent it works at all – it only works for DGFIP. The matching of *purchases* by Firm "B" with sales reported on the VAT return of Firm "A" cannot be done. There is no EU Purchases List, only an EU Sales List – the VIES.

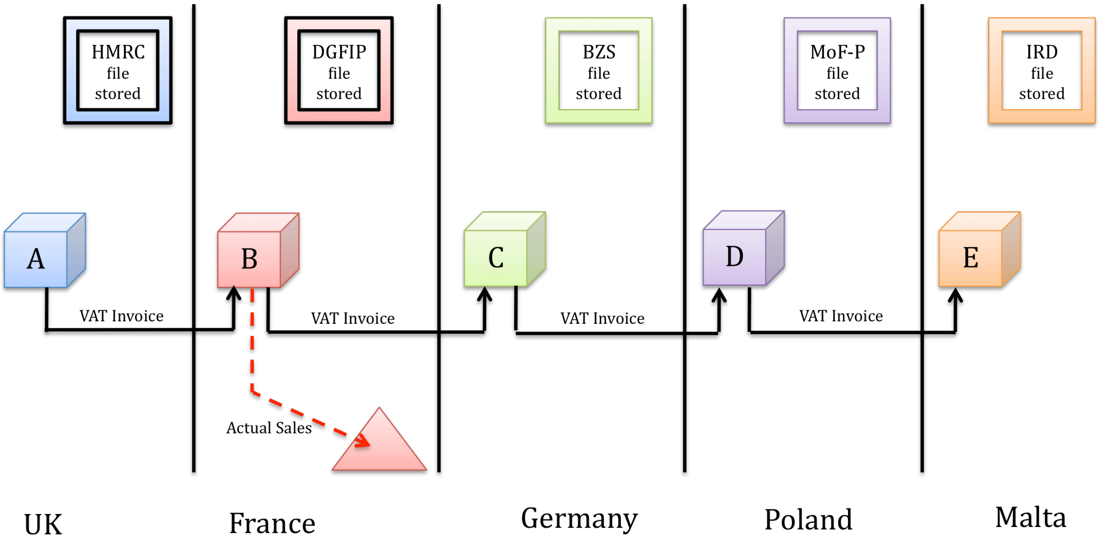
Example 2 (Buffer companies)

Assume that Firm "A" in the UK agrees to sell a specific quantity of identified high-value goods to firm "B" in France. The price is set. The time and method of delivery are also agreed. Firm "A" plans to zero-rate the sale and recover the input VAT. Firm "B" is expected to perform a reverse charge in France.

Assume further that the fraudsters have established a series of shell companies in Germany, Poland and Malta so that the goods that Firm "B" purchases from Firm "A" can be re-sold to Firm "C" (Germany),[65] then sold again to Firm "D" (Poland),[66] and finally to Firm "E" (Malta).[67]

Finally, assume that the goods arrive in France from the UK, but never leave. They are actually sold in the French market and VAT is charged, but not reported. On its return Firm "B" shows a reverse charge (as expected), but it also shows a zero-rated intra-community supply to Firm "C" with little or no net tax due. The fraudsters' intent is for Firm "B" to escape detection in France for a period of time and then disappear if and when the authorities begin to audit the transactions. Assume that Firms "C" (Germany), and "D" (Poland) file returns with little or no net VAT due, but Firm "E" (Malta) does not file. The assumption of the fraudsters in this case is that it is easier to escape detection in Malta than elsewhere in the EU. See: Figure 5.

Figure 5



Traditional MTIC detection through VIES. The traditional method for detecting this fraud relies upon the Maltese Inland Revenue Department identifying that Firm "E," which has a valid Maltese VAT ID, but which does no business in Malta, is a fraudster.

[65] The Federal Central Tax Office is the *Bundeszentralamt für Steuern* (BZS).
[66] The Ministry of Finance is the *Ministerstwo Finansów* (MoF-P).
[67] The Inland Revenue Department of the Ministry of Finance (IRD).

If Firm “E” does no real business in Malta, if it does not take possession of the goods purchased from Firm “D” (Poland), sells nothing, does not perform a reverse charge, and files no returns, then it may be difficult for Malta to find (or suspect) this fraudster.

Under the current system the way that Malta would be expected to find this fraud is through VIES reports. If Firm “D” (Poland) reported properly, then its recapitulative statement would record an entry for sales made to Firm “E” (Malta). If the Maltese Inland Revenue Department (IRD) suspected fraud it would request assistance from the *Ministerstwo Finansów* (Ministry of Finance – Poland – [MoF-P]), and then further to the *Bundeszentralamt für Steuern* (Federal Central Tax Office – Germany – [BZS]), and finally to the DGFIP.

If a VIES request takes four months at a minimum to generate a response, then it may be well over a year between the time of the Maltese initiative and the moment when the DGFIP is alerted that there may be a fraudster selling goods into the French market. If the fraudsters are good at their trade, then there will be a considerable number of “early warning” signals that something is amiss. These will come as tax inspectors show up at the various business locations in Malta, Poland and Germany looking for registered companies, and discovering mere shells.

MTIC detection through the proposed Third Invoicing Directive. Under the proposed Third Invoicing Directive this fraud could be detected in France through a risk assessment program performed entirely within the DGFIP.

Under the fact pattern presented, the DGFIP has the complete invoice data for the sale of goods from the UK seller (Firm “A”) to the French buyer (Firm “B”), as well as the complete invoice data for the sale from France (Firm “B”) to Germany (Firm “C”). The invoices can be matched. It should be standard practice under DGFIP risk assessment to notice that all of the purchases from Firm “A” have been re-sold to Firm “C.”

There is nothing inherently wrong with being a middleman, but one might expect that the goods would pass directly from Firm “A” to Firm “C” in a triangular sale, rather than going from the UK to France, and then on to Germany. But there is more. A risk assessment program would have the invoice prices. A measure of the commercial mark-up could be taken. (A common indicator of MTIC fraud is low margin/no margin sales.) But, this may still not be enough.

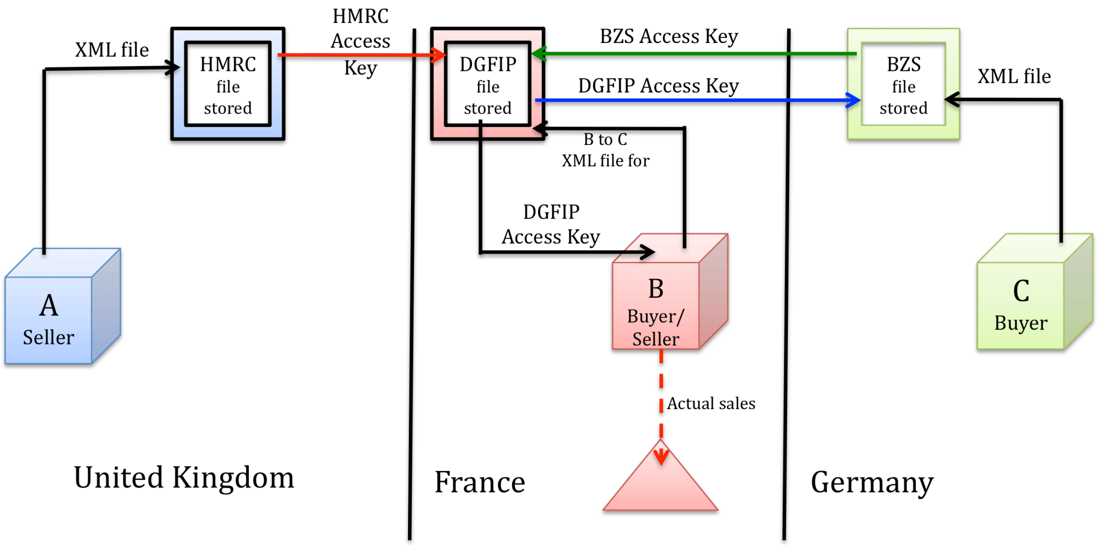
It is clear that the BZS (Germany) is doing exactly what the DGFIP (France) is doing. However, the BZS is looking not only at the sale from France (Firm “B”) to Germany (Firm “C”), but it is looking at the sale from Germany (Firm “C”) to Poland (Firm “D”). If it turns up that the same goods are being sold, and re-sold with very small margins in multiple sales across the Single Market, then there is a very strong suggestion that MTIC fraud is present. Automated warnings should start to go off in the office of the

DGFIP or the BZS. MTIC transactions are not commercially rational, and the easiest way to detect them is to measure them against commercial standards.

The solution. Denying further "requests for authorization" will stop *future* sales. This is a simple matter of refusing to issue access keys until the traders involved are able to clarify their transactions. Both DGFIP and BZS might refuse to issue more access keys until the issues raised here are cleared up.

Furthermore, VAT invoices that have *already been issued* by any of the firms in the chain could be digitally extinguished *after the fact*, if the related returns had not been filed. A document purporting to be an invoice under the proposed Third Invoicing Directive is not a VAT invoice if it does not have two valid access keys. Figure 6 shows the access keys that DGFIP has at its disposal to make this assessment.

Figure 6



CONCLUSION

MTIC/MTEC fraud has risen to levels where it can no longer be ignored. The VIES is neither adequate to deal with it, nor is it able to adapt as MTIC/MTEC morphs into new forms of fraud and enters into new marketplaces. The fundamental problem with the VIES as a MTIC/MTEC enforcement tool is that the fraud is fast, but the VIES is slow. VIES data is months out of date by the time it is applied. It is an aggregate data system that provides granular answers only on special *request*.

There is a better way. That way is technology-intensive, but it is not technologically heavy. It involves placing digital signatures on invoices and then feeding invoice-data back into relational databases that match transactions and perform risk assessments across the Single Market. Data is shared in advance. It is shared automatically among the jurisdictions that are parties to a specific transaction and allows local enforcement against local losses.

Because this proposed Third Invoicing Directive works at a granular level, in advance of the VAT invoice, it identifies fraud patterns early, and prevents revenue losses even after the fraud starts. From a workability perspective the Brazilian SPED demonstrates that this kind of digital control over invoice data works to solve cross-border fraud. Compliance is no more burdensome than swiping a credit card and waiting for approval.

This solution is not just another modification of the VIES. It is a much more fundamental modification of the Invoicing Directive. Recapitulative statements and the VIES can never provide real-time enforcement.