

# Technology Can Solve MTIC Fraud – VLN, RTvat, D-VAT certification

**Technology can solve missing-trader intra-Community (MTIC) fraud. In the early 2000s, MTIC fraud mainly concerned cell phones and computer chips. By 2006, MTIC fraud was targeting services (transfers of CO<sub>2</sub> permits and VoIP services) and was no longer limited to the European Union. MTIC fraud is now fully digitized (the supply, the movement of the product and the funding). Technology is both the causative agent and the most effective countermeasure for this type of fraud. The details of the three major technology-intensive approaches for solving MTIC fraud are known since 2007: the VAT locator number (VLN); real-time VAT collection (RTvat); and certified tax software (Digital VAT or D-VAT). This article endeavours to contribute to the debate that the European Commission has opened on this topic with its recent Green Paper, by comparing and contrasting these proposals.**

## 1. Introduction

Technology can solve missing-trader intra-Community (MTIC) fraud.<sup>1</sup> This should come as no surprise. MTIC fraud is technology-intensive fraud – its solution should also be technology intensive. Missing-trader fraud arises when a business purchases goods or services (tradable rights) without having to pay VAT to its supplier, collects VAT from its customer on the subsequent supply, and then disappears without having remitted the tax to the tax authorities. Businesses can easily avoid paying VAT on their inputs if their purchases are taxed on the basis of an intra-Community acquisition of goods, under the reverse charge mechanism (in respect of cross-border services) or under postponed accounting (on the importation of goods).<sup>2</sup> Those mechanisms work very well where the customers or importers are honest businesses but they also enable dishonest businesses (fraudsters) to derive maximum profit from missing-trader fraud.

In the early 2000s, when MTIC fraud mainly concerned cell phones and computer chips, newspaper reporters visited fraudsters and got lessons on how easy it was to turn the carousel<sup>3</sup> – provided that you had a laptop.<sup>4</sup> At that time, MTIC fraud was in the process of morphing from a fraud that involved the physical movement of goods across the borders of the European Union to a fraud that was primarily a function of technology. The goods – if the fraudulent transactions actually concerned existing goods – would stay in a warehouse<sup>5</sup> and the fraud would be carried out by merely exchanging invoices through laptops.

By 2006, MTIC fraud had morphed again.<sup>6</sup> Now, MTIC fraud was targeting services (transfers of CO<sub>2</sub> permits and VoIP services). Once again (after it was uncovered), newspapers carried stories explaining that it was even easier to carry out this variant of MTIC fraud. In these cases, the supplied product itself (the CO<sub>2</sub> permits or VoIP minutes) was digital. Fraudsters on the BlueNext exchange reportedly worked their frauds from laptops in the comfort of Parisian cafés.<sup>7</sup> With the attack on services, MTIC fraud also became an “international” fraud.<sup>8</sup>

\* Adjunct Professor, Boston University School of Law.

1. Apart from the fact that the term “Community” is no longer appropriate (under the Treaty of Lisbon, the term has been replaced by “European Union”), “MTIC” has become an outdated term. Now that missing-trader fraud has moved into services, it is no longer confined to intra-Community trade in goods. Norway is just as concerned about missing CO<sub>2</sub> traders on the Nord Pool, as are the French about these same “traders” on the BlueNext, and the Italians on the GME (*Gestore Mercati Energetici*). If we wish to stay with the older acronym, it should be adjusted to MTIC/MTEC fraud (with MTEC standing for missing-trader extra-Community).
2. The three mechanisms have in common that, instead of paying VAT to their suppliers, customers (importers) are legally required to account for VAT through their periodic VAT returns on the value of the goods and services received or imported from abroad. In practice, the customers and importers can easily escape from their legal obligations.
3. MTIC fraud is also known as carousel fraud because, in specific scenarios, the same goods go around in circles; the goods are traded many times among the same parties.
4. Ashley Seager and 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*, 9 May 2006, available at: <http://www.guardian.co.uk/uk/2006/may/09/ukcrime.ashleyseager>:  
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.”
5. However, under the judgment of the Court of Justice of the European Union (ECJ) of 27 September 2007 in *Teleos, Plc and Others v. Commissioners of Customs and Excise*, Case C-409/04, [2007] ECR I-7797, in order to be zero rated, the intra-Community supply must concern real goods and those goods must physically have left the Member State of origin.
6. 2006 is a rough estimate for the morphing into services. It may have been earlier, but undetected. The VoIP fraud uncovered in 2010 at Fastweb and Telecom Italia began at this time. See Richard T. Ainsworth, “The Italian Job – Voice-Over-Internet-Protocol MTIC Fraud in Italy”, 58 *Tax Notes Int'l* 721 of 31 May 2010. CO<sub>2</sub> trade began on 1 January 2005. In December 2009, Europol said it had been tracking this mutation for 18 months, so this strain of MTIC fraud dates back at least to 2007. See Richard T. Ainsworth, “CO<sub>2</sub> MTIC Fraud – Technologically Exploiting the EU VAT (Again)”, 57 *Tax Notes Int'l* 357, 25 January 2010.
7. Aline Robert, “La fraude a la TVA du CO<sub>2</sub> se revele gigantesque”, *La Tribune* 22 of 16 December 2009 (in French, original and translation on file with author):  
With the accessibility of Bluenext and effectiveness of the platform, which allows regulatory delivery in 15 minutes, fraudsters indeed have a place where they can place orders on millions of tons of CO<sub>2</sub> while quietly installed in their Parisian cafés. Using temporary Internet addresses on sites like Yahoo! or Gmail also makes it easier for crooks. The cases reveal a crying absence of regulation in the CO<sub>2</sub> market.
8. Richard T. Ainsworth, “VAT Fraud: The Tradable Service Problem”, 61 *Tax Notes Int'l* 217 of 17 January 2011 (discussing the morphing of MTIC into MTEC fraud and introducing the expression).

Enforcement also shifted. Tax authorities began to follow the funds. For example, in the United Kingdom, the tax authorities discovered that most of the money they were chasing had been transferred between accounts at the same offshore bank: the First Curaçao International Bank (FCIB). FCIB was shut down.<sup>9</sup>

Fraudsters responded and, predictably, the response was digital. Internet payment platforms<sup>10</sup> were developed and became the preferred method for moving the huge sums of money that backed the frauds. These platforms are immune from traditional banking oversight, operate outside normal channels, and are difficult to shut down with funds remaining within.

MTIC/MTEC fraud was now fully digitized (the supply, the movement of the product and the funding). The consequences should be clear. MTIC/MTEC fraud must be *prevented* (before the fact), not *pursued* (after the fact). In the digital world, everything evaporates when pursued. Technology is both the causative agent and the most effective countermeasure for this type of fraud.

We have known the details of the three major technology-intensive approaches for solving MTIC/MTEC fraud since 2007: the VAT locator number (VLN);<sup>11</sup> real-time VAT collection (RTvat),<sup>12</sup> and certified tax software (Digital VAT or D-VAT).<sup>13</sup> This article endeavours to contribute to the debate that the European Commission has opened on this topic with its recent Green Paper,<sup>14</sup> by comparing and contrasting these proposals.

## 2. Technology Solutions

There are important differences and similarities between the VLN, RTvat and D-VAT certification proposals.

VLN enables the tax authorities to track individual transactions, whereas RTvat focuses on securing the VAT element of every payment. D-VAT certification differs in both respects. It achieves a secure VAT remission system through certified tax software and trusted third parties. These third parties are service providers that stand between businesses and tax authorities, file the VAT returns for the businesses, and remit the VAT due by their clients – guaranteeing the accuracy of the return and the payment of the tax due.

There is a considerable amount of central control under both the VLN and RTvat proposals. Central (government) computer systems will track each transaction (VLN) or payment (RTvat). Under D-VAT certification, there is no central tracking, just assurance that each trans-

9. Ian Cobain and Ashley Seager, "Carousel fraud: Follow the Money: the multibillion pound trail that led to Caribbean bank: Customs investigators found suspected fraudsters had one thing in common: accounts at same institution", *The Guardian* of 21 September 2006; "First Curacao International Bank NV Subject to the Emergency Measure", Press Release 06-013 of the First Curacao International Bank of 11 October 2006 (indicating that "... as a result of several criminal investigations in relation to VAT fraud involving a large number of customers, and subsequent attachment of funds, FCIB has come into a position in which it no longer is able to process payments, ...") available at: <http://www.firstcuracao.com/index.html>.

10. The press is ahead of tax enforcement with respect to online payment platforms. In CO<sub>2</sub> MTIC/MTEC fraud, these platforms register on an exchange (recently the Danish exchange has been popular) and hold a single large account with a traditional bank, but take deposits and make transfers for traders (normally for EUR 500 whereas a traditional bank would charge EUR 30 for an international swift payment). The transfers are invisible to the normal banking systems as long as the funds remain in the carousel. The platforms are removed from the Internet when they become part of an inquiry. See, for example, First Bancorp Ltd:

First Bancorp Limited (FBL) provides you an online payment solution that is based in New Zealand. FBL can provide B2B commercial and private banking services with no restrictions to a worldwide customer base.

[Text from the First Bancorp Ltd. web site <http://fblimited.com> which has since been removed from the Internet, but can be seen preserved on a business locator site <http://www.aboutus.org/fblimited.com>]. First Bancorp Ltd. was removed from the Danish exchange in the first round of "clean-up" following press investigation after the Europol announcement of fraud on the Danish exchange [Europol Press Release, *Carbon Credit fraud causes more than 5 billion euros damage for European Taxpayer* (9 December 2009) available at: <http://www.europol.europa.eu/index.asp?page=news&news=pr091209.htm>].

Experimenting with this process, Bo Elkjaer and John Mynderup (journalists with *Ekstra Bladet*) made contact with the Director of Swefin, Anders Garbro. Bo Elkjaer and John Mynderup, *Anders Garbro: Jeg svindler ikke med CO<sub>2</sub>* (Anders Garbro: I do not tamper with CO<sub>2</sub>), *Ekstra Bladet* of 3 December 2010 [in Danish, translation on file with author]. Garbro initially acknowledged his "shadow banking" operation, which is necessary because "... the transactions just go fast. It's not like the banks where transactions can take a long time." Garbro read the published account in *Ekstra Bladet* of Friday 3 December 2010, called another Director of the company, Kashif Ghaus Qadri, who had lived in Ishoej, Denmark, but recently moved to Dubai, United Arab Emirates.

On the night of Friday [3 December 2010], the Internet bank Swefin Online vanished without a trace from the surface of the earth. The online bank has played a central role in the massive fraud in CO<sub>2</sub> allowances in the scandal that has hit the Danish quota registry.

Bo Elkjaer and John Mynderup, "Dansk Kvotesvindler I Luksus I Dubai", (Danish Quota Fraudster [Living in] Luxury in Dubai), *Ekstra Bladet* of 6 December 2010 [in Danish, translation on file with author]. Unfortunately, closing an Internet payment platform does not have a significant impact on CO<sub>2</sub> fraud as there are hundreds of similar platforms, platforms constructed on top of other platforms, with more platforms ready in the wings to move in, assume control of funds and continue business as usual. Making an Internet payment platform disappear is much easier for fraudsters than closing an offshore bank, like FCIB.

11. VLN was formulated and proposed by Dr Michael Cheetham at the House of Lords hearings on 25 May 2007. House of Lords, European Union Committee, "Stopping the Carousel: Missing-Trader Fraud in the EU" (Report with Evidence), HL Paper 101 of 25 May 2007, p. 78-82; Michael Cheetham, "For who so firm that cannot be seduced? (2007 PowerPoint presentation) at 20-23; 29-34 (on file with author).
12. Charles Jennings, "The EU VAT System – Time for a New Approach?" *International VAT Monitor* 4 (2010); further details are available at: <http://www.rtvat.eu/>.
13. See Charlene-Adline Herbain, "VAT Fraud on Carbon Allowances", *Tax Planning Int.* – *Indirect Taxes* of 4 September 2009 (suggesting that the Commission should follow the software certification provisions of the American Streamlined Sales Tax Initiative); Richard T. Ainsworth, "MTIC Fraud Infects Tradable Carbon Permits", 55 *Tax Notes Int'l*. 733 of 31 August 2009 (setting out a targeted solution to MTIC fraud in the CO<sub>2</sub> market); Richard T. Ainsworth, "Car Flipping in the UK – The VAT Fraud Marketplace and Certified Solutions", 47 *Tax Notes Int'l*. 1157 of 24 September 2007 (assessing the car-flipping VAT fraud in the United Kingdom to MTIC fraud and proposing a limited certified software solution); Richard T. Ainsworth, "Tackling VAT Fraud: Car Flipping and Computer Chips on a Carousel", 46 *Tax Notes Int'l*. 267 of 16 April 2007 (comparing car-flipping fraud in Canada with MTIC fraud in the United Kingdom and proposing a certified software solution); Richard T. Ainsworth, "Tackling VAT Fraud: 13 Ways Forward", 45 *Tax Notes Int'l*. 1205 of 26 March 2007 (assessing and comparing many of the most viable solutions for MTIC fraud and further proposing a fully digital solution); Richard T. Ainsworth, "Carousel Fraud in the EU – A Digital VAT Solution", 42 *Tax Notes Int'l*. 443 of 1 May 2006 (setting out a fully digital solution for MTIC fraud).
14. European Commission, "Green Paper: On the Future of VAT – Towards a simpler, more robust and efficient VAT system", COM(2010) 695/4 of 1 December 2010. The Green Paper launches a wide consultation process with all stakeholders on the current VAT system and the possible ways to strengthen and improve it. The consultation will continue until 31 May 2011. On the basis of the feedback received, the Commission will draw up a Communication before the end of 2011, setting out the priorities for a future VAT strategy.

action is completely and accurately reported because the tax reporting systems are certified and guaranteed.

Finally, both VLN and D-VAT certification go to great lengths to avoid making fundamental changes in the way the EU VAT system currently operates (VLN perhaps even more than D-VAT certification). Apart from the fact that it is presented as an origin-based VAT system, the RTvat proposal requires amendments to the current EU VAT system as regards the time the tax becomes chargeable and deductible. In this respect, it should be noted that RTvat also works very well as a destination-based system.

It is clear that missing-trader fraud can only effectively be prevented EU-wide if the systems are compulsory for all businesses.

## 2.1. VLN

The VAT Locator Number (VLN) system<sup>15</sup> is the simplest of the three technology solutions. It is the least disruptive to the current EU VAT system and is very targeted. It is *only* looking at preventing MTIC/MTEC fraud.

The most significant policy change made by the VLN proposal is the denial of a customer's right to deduct input tax if the VAT is mentioned on an invoice without a valid VLN. The most significant procedural change is that businesses will be required to secure a valid VLN, and attach it to an invoice (when they make a domestic or cross-border supply of goods or services).

In most cases, both sides of this compliance measure will be fully automated. Accountancy software platforms will make automated *requests* for VLN from a central (government) computer system, and make automated *validation checks* in the same manner. Each link in the commercial chain will be given a number, and the numerical sequence will follow the goods (or services) from initial production until final consumption. A backup system where VLN are secured through an Internet website or a call centre will be available.<sup>16</sup>

The VLN system requires the supplier to secure and print on the invoice for each transaction an encrypted VLN. This number will be unique to a specific transaction (based on the essential data elements of the invoice, and prior related VLN from transactions up the commercial chain). The VLN will be attached to the invoice, either numerically or as a bar code that can be scanned and read with an optical reader.<sup>17</sup> The advantage of a bar code and optical reader capabilities is that a trader can quickly scan the VLN in order to verify its validity through a national database.

A similar fraud prevention system is in place in Brazil, where it has proven to be highly reliable against a different type of cross-border fraud.<sup>18</sup> In Brazil, invoices relating to interstate transactions receive a digital bar code at the internal border from a federal computer feed. The bar code validates the invoice and the destination of the goods.<sup>19</sup>

The following example clarifies how VLN works within the European Union.

## Example

If business A in the United Kingdom supplies goods or tradable services to business B in France, A will zero rate<sup>20</sup> the transaction. A will request a VLN from the UK tax authorities' central computer system. The number returned will be VLN-1.

VLN-1 includes the essential elements of A's invoice. The UK tax authorities will perform a risk assessment (based on A's compliance history, the size of the present transaction, and some criteria as to whether or not the transaction is "normal" for A). If they find that A is a "low-risk exporter", the tax authorities will issue VLN-1.

B will then account for French VAT on the intra-Community acquisition of the goods.<sup>21</sup> When B seeks to make an onward supply (to C in France) of all or some of these goods, B will request a new VLN for the subsequent transaction. In that framework, B will submit all the essential attributes of the invoice, which include a copy of VLN-1. If this request passes the French tax authorities' risk assessment, a new number will be issued (VLN-2).

B must place VLN-2 on the invoice.<sup>22</sup> When it receives the invoice from B, C should not pay the amount of VAT to B until it has verified the validity of VLN-2. If it pays the VAT to B without checking VLN-2, then C will be at risk of being denied the right to deduct the VAT if the VLN on the invoice turns out to be invalid or if the invoice does not contain a VLN at all.

Since VLN-2 includes not only data from the transaction between B and C, but also data from the transaction between A and B, the tax authorities will be able to reconstruct the full commercial chain. Because C will be on notice that its right to deduct is in

- .....
15. House of Lords, see note 11.
  16. Dr Michael Cheetham, personal e-mail communication of 25 April 2010 (on file with author).
  17. A similar bar code is added to each electronic cash register (ECR) receipt issued by Quebec restaurants under the tax authorities' enforcement effort directed against "zappers". The sales recording module (SRM) is a device that secures ECR data and uses it to digitally sign each receipt with a bar code that can be read with a hand-held optical scanner. This will allow short inspections – where, in a 30-minute visit, an auditor observes that customers are receiving receipts, and then quickly verifies (with the scanner) that the receipts being issued have been recorded in the SRM. Full inspections can follow in cases of irregularities. Gilles Bernard, *Solutions for the Underreporting of Income in the Restaurant Sector*, Federation of Tax Administrators Annual Conference, Denver, Colorado, 2 June 2009, PowerPoint slides Nos. 15-17 (on file with author).
  18. The Brazilian problem is that goods crossing from one state into another occasionally get separated from the invoice. The invoice continues along the commercial path while the goods avoid border controls and "circle back" into the state from which they came where they are sold (with tax) to consumers. The businesses involved effectively secure a deduction in the state where the goods were (allegedly) exported, and collect the tax in the state from which the goods were (allegedly) "exported". The digital bar codes on the invoice allow the tax authorities to make sure that the specific goods that were supposed to have crossed the border actually arrive with the invoice. This is an intra-state permutation of the familiar export VAT fraud found elsewhere. See Louis and Marlene Botes, "Money-Laundering in South Africa", *International VAT Monitor* 4 (2002), p. 258.
  19. A number of Brazilian states and the federal government signed an agreement on 30 September 2005 to introduce "e-invoicing" (*Nota Fiscal Eletrônica*) and the "auxiliary document of the e-invoice" (*Documento Auxiliar da Nota Fiscal Eletrônica*), *Ajuste Sinief* No. 07 of 30 September 2005. On 20 December 2005, through ATO COTEPE/ICMS No. 72 of 20 December 2005, the structure of the e-invoice was established, and testing was initiated with 19 companies and 6 states. The programme was considered to be a success and has been extended.
  20. In the case of services, UK VAT will not apply because the place of supply will be in France.
  21. In the case of services, B will account for VAT on the value of the services, under the standard reverse charge mechanism.
  22. Where the onward supply consists of multiple purchases, two avenues are available: either separate invoices are issued for each part of the supply (each with a discrete VLN), or an aggregate invoice could be issued (with an aggregate VLN). This issue was not addressed in the House of Lords, but has been answered by Dr Cheetham independently. Personal e-mail communication, Dr. Michael Cheetham of 23 January 2011 (on file with author).

jeopardy if it does not check the validity of VLN-2, the system will become self-enforcing with a known penalty, not just self-enforcing as a matter of good accounting practice.

Due diligence under this regime is directed at the VLN (not at the more difficult to assess commercial/financial profile of the commercial parties in the chain).<sup>23</sup> If VLN-2 is confirmed as being a valid number, C will be assured that it can deduct the VAT it has paid to B. If there is any suspicion on the part of the tax authorities that the transaction is irregular, the authorities can prevent C from paying the VAT to B or, if C has paid it, prevent C from deducting it, by rejecting the VLN request. This rejection will not necessarily stop the commercial transaction, but supplier and customer would be on notice that some other arrangement for payment of the VAT is needed.

When there is a VLN irregularity, the automatic response of the next trader in line is to pay the supplier the VAT-exclusive price for the supply and to pay the VAT directly to the tax authorities.<sup>24</sup> The VLN system will allow this payment, and the tax authorities will send a receipt to both parties. This is probably the only action that will allow the customer to quickly secure a follow-on VLN for re-supplying the goods or tradable services. Since no deductible VAT is ever paid to a business that makes supplies without a valid VLN, missing-trader fraud is eliminated.

One of the difficulties with the VLN is its granularity. VLN associates each good and each service with a discrete number, as the intention is to follow a specific cell phone, or computer chip through the entire commercial chain. Theoretically, an individual cell phone sold by a retailer could be traced back to a batch at a wholesaler, and then to the shipping container at the distributor's warehouse, and further to the lot number at the manufacturer. However, each cell phone contains parts (at least a chip and a SIM card) that would also have a chain of VLN numbers that would necessarily be integrated with the cell phone's VLN as it passed through the commercial chain.

The granularity of the VLN system may turn out to be extremely cumbersome, not only at the production stage but also at the subsequent stages of distribution of the final products, especially where a transaction concerns standard products that the supplier has purchased from various sources and that he has stored together in a large tank, container or silo, or where the supply concerns a number of goods purchased from various sources. The VLN system may require that individual goods and services have their own VLN numbers which must be traced by subsequent suppliers. As regards bulk products, it may be practically impossible to determine from which purchase the resupplied goods originate. As it will not be possible to digitize in this manner all goods and services circulating in the entire economy, the VLN system may have to be limited to selected suspect parts of the market.

It is also unclear how effectively the tax authorities can carry out the risk assessment in the process of deciding whether or not they will issue a VLN.

## 2.2. RTvat

In some respects, RTvat is born out of the same insights as VLN. The application of the VAT withholding mechanism is, however, not limited to "suspect" transactions but will become the new standard.

Unlike VLN, which digitally tags each supply and penalizes traders who pay VAT to their suppliers without having a valid VLN, RTvat digitally sequesters each payment that includes a VAT component and simply eliminates the possibility for the supplier to receive the VAT from his customers.

RTvat makes two significant structural changes to the VAT system, along with a dramatic procedural adjustment. Firstly, it changes the supplier's VAT liability to the date on which he receives the price from his customer, and the customer's right to deduct input tax shifts in tandem to the date on which he pays his suppliers.<sup>25</sup> The supplier's liability itself is unchanged. Only the collection of the tax changes: it is automatically linked to settlement of the transaction by the customer. Secondly, RTvat (as proposed) is an origin-based tax system, which is a logical consequence of the fact that, under Art. 402 of the VAT Directive,<sup>26</sup> the "origin system" is still envisaged as the "definitive system" for VAT in the European Union. However, RTvat could just as easily be destination based.

The procedural change is the most striking attribute of RTvat.<sup>27</sup> Under RTvat, suppliers only receive the VAT-exclusive price for their supplies. The VAT element is automatically split off from the customer's payment and is separately (electronically) remitted to the tax authorities by the supplier's bank, which makes it necessary that the transaction is paid by means of electronic funds transfer (EFT). Through EFT, the tax authorities can refund the deductible VAT to the customer on the same day they received it from the supplier's bank.<sup>28</sup>

23. Due diligence requirements are set out in the judgment of the ECJ of 6 July 2006 in *Axel Kittel v. Belgian State and Recolta Recycling SPRL v. Belgian State*, Joined Cases C-439/04 and C-440/04, [2006] ECR I-6161. They essentially require purchasers to examine whether their counterparty is likely to be engaged in fraud:

... where it is ascertained, having regard to objective factors, that the supply is to a taxable person who *knew or should have known* that, by his purchase, he was participating in a transaction connected with fraudulent evasion of value added tax, it is for the national court to refuse that taxable person entitlement to the right to deduct.

24. This withholding mechanism is in fact the operating principle of RTvat. However, unlike RTvat, the withholding mechanism only applies in incidental cases.

25. Information brochure "RTvat: An Introduction to a Real-time Solution for Improving the EU VAT System" of 5 March 2009.

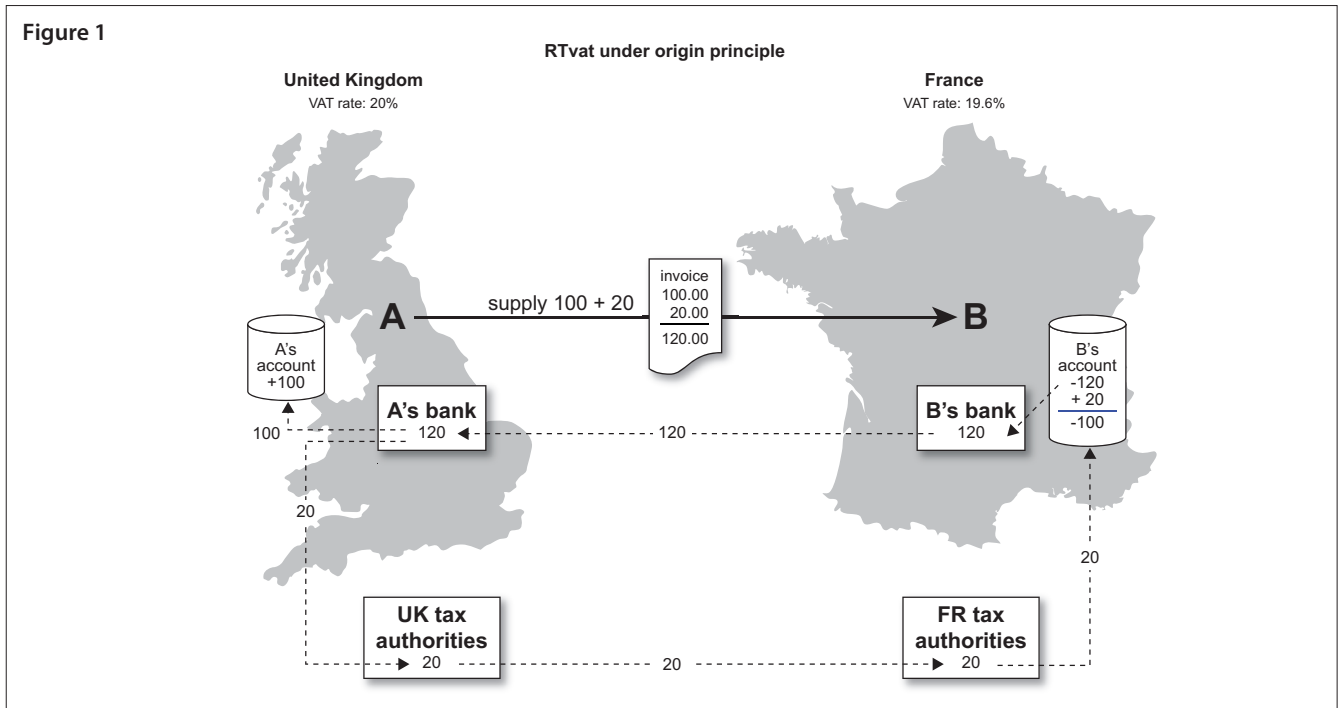
26. Jennings, see note 12, p. 257.

27. The RTvat system also includes "a sophisticated fraud analysis tool, based on analytical applications currently used in the credit card and financial services arenas".

28. As a settlement-based system, cash and cheque payments delay the refund mechanism, because they delay the VAT payment to the tax authorities. Jennings, see note 12, at 258 notes:

Where the supplier is paid by cheque or cash, the tax component should be remitted to the tax authority no later than the time when the non-tax part (of the payment) is banked. The VAT on cash transactions is captured when the supplier transfers his takings to his bank account; ...

Figure 1



RTvat borrows the payment system of the credit card industry and applies it to VAT collection.<sup>29</sup> Also payments made by final consumers to retailers by means of credit or debit cards, or other types of “plastic money” or by means of mobile telephones are split up and the VAT element is directly remitted to the tax authorities.<sup>30</sup> If all Member States were to adopt the RTvat system, a network of 27 identical linked servers (one in each Member State) would act as communications and fund transfer centres. Each Member State would own and operate its own server and all domestic and intra-Community transactions would be processed through it.

Under RTvat, missing-trader fraud is virtually impossible because no business ever holds, on behalf of the government, any VAT received from a customer. It is impossible for the supplier to go “missing” with the VAT in hand, except in the case of retail transactions for which the customer pays in cash (not by means of credit card or other kind of “plastic money”).

On the basis of a supply made by business A in the United Kingdom to customer B in France for a VAT-exclusive price of 100, RTvat’s original proposal, which is based on the origin system, can be visualized as follows (see Figure 1).

The RTvat collection mechanism would even be more efficient if it were based on the destination principle (see Figure 2) and the customers’ payments were split up by the customer’s bank. This solution would prevent the tax authorities of a Member State from having to refund the VAT to a customer established in another Member State. If applied under the destination principle, RTvat requires that suppliers making cross-border supplies know the VAT applicable in their customers’ Member States. That should not be a serious problem and, if it is difficult to determine whether the supply is subject to the standard or a reduced rate in the Member State of destination, the

supplier could simply charge the standard rate in B2B relationships, because the customer can deduct the VAT anyway. The potential disadvantage of the destination principle is that businesses may have to file multiple VAT returns in multiple Member States. However, it should not be necessary for businesses to file a VAT return in respect of transactions paid through the designated bank payment channels and processed by the tax authorities.

Although RTvat can in principle be applied EU-wide, it may be wise to exclude transactions with a low value and those subject to the margin scheme from the compulsory system.

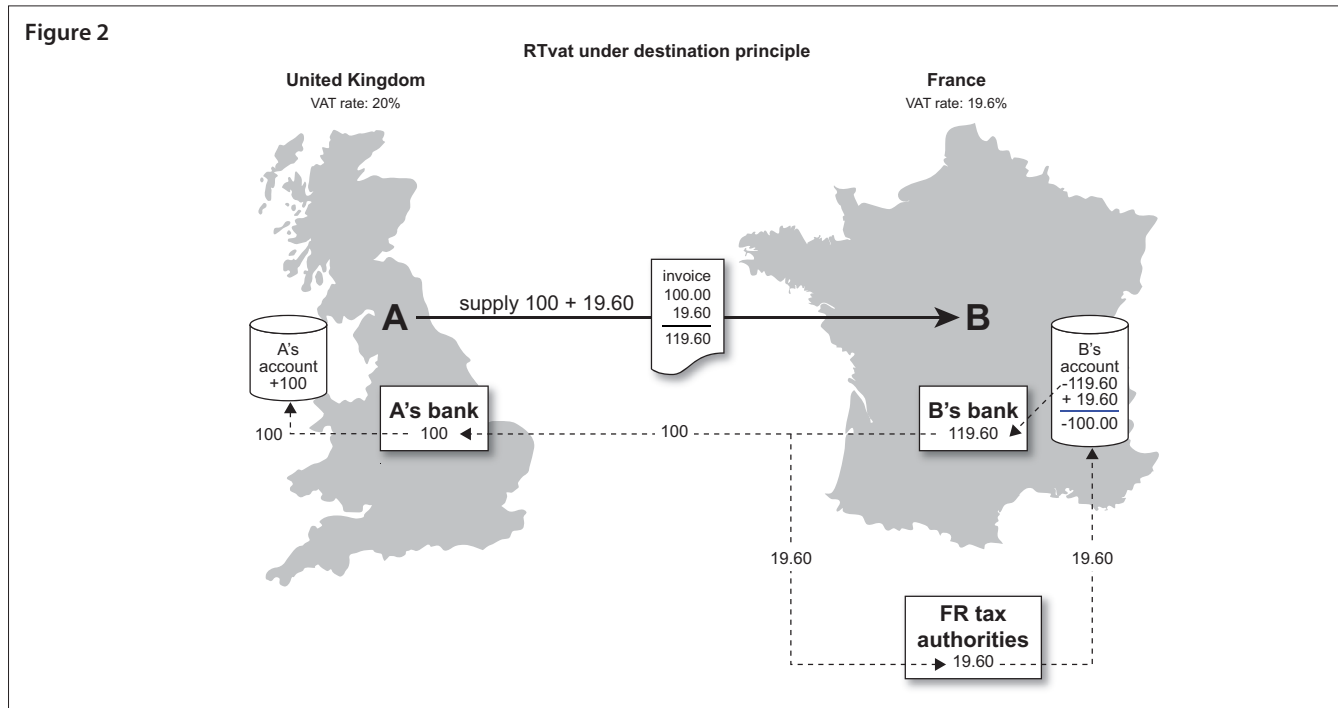
If RTvat had stopped at this point, the system would be striking for its simplicity, originality and workability.<sup>31</sup>

29. A number of jurisdictions outside the European Union have rules very similar to RTvat, but apply them only when payments are made by credit/debit cards. In Ecuador, all credit/debit card payments for taxable purchases require the credit card company to remove 30% of the VAT and remit it directly to the tax administration (Art. 63 of the VAT Act and Regulations 118-120). Colombia has a similar law, but the amount remitted is 75% of the VAT on all payments made with credit/debit cards (Art. 437(1) of the VAT Act). In Mexico, the withholding amount is 100% of the VAT and the remission to the tax administration is immediately on payment, however, the withholding is done by the purchaser, not by credit card companies.

30. Jennings, see note 12, at 257 notes:

The key change in moving to real-time collection of VAT is that the tax is collected and remitted on each individual transaction at the time the customer settles payment of the transaction with the supplier. For B2B transactions settled by electronic funds transfer between customer and supplier, the tax element contained in the payment would be separated by the payment service provider and remitted directly to the tax authorities.

31. It is important to note, however, that much of what the RTvat does has been considered in the “Mittler Model”, which was developed and presented in 2003 at the Tax Policy Conference, *Value Added Tax Evasion and Model Approaches for its Avoidance*, of the Ifo Institute for Economic Research, available at [http://www.cesifo-group.de/portal/page?\\_pageid=36,385339&\\_dad=portal&\\_schema=PORTAL&item\\_link=steuer-gemeinschaftskonferenz-2003-bericht.htm](http://www.cesifo-group.de/portal/page?_pageid=36,385339&_dad=portal&_schema=PORTAL&item_link=steuer-gemeinschaftskonferenz-2003-bericht.htm) (English and German). The central difference between RTvat and the Mittler Model is that the Mittler Model works with exemption certificates instead of money. There is no banking system involvement under the Mittler Model. The Mittler Model is therefore much less expensive to operate but it is contrary



RTvat not only effectively prevents missing-trader fraud<sup>32</sup> but also combats other types of fraud, including suppression fraud.<sup>33</sup>

However, the RTvat proposal goes further. The system for splitting up payments is not based on the related invoices. Instead, RTvat derives the necessary information from the supplier's business records, which means that part of the supplier's business records is audited on every occasion the supplier receives payment for a transaction. To that end, the computer system is equipped with the Tax Authority Settlement System (TASS).<sup>34</sup> In that respect, RTvat may overreach. It may get caught in data collection and security issues that it may not be able to address.

There are many unanswered questions about the scope and content of the data in the TASS. Specifying the VAT identification numbers of both parties and identifying all intra-Community transactions is a long way from the 320 data points in the OECD's Standard Audit File – Tax<sup>35</sup> (SAF-T), which the OECD believes is necessary for quality remote audit and fraud detection. If RTvat gathers SAF-T quality data from all EU businesses, it faces two data security issues: it will need to guarantee that its data has not been tampered with before it arrives, and it will need to protect its data against external attacks while it is retained and transmitted. The RTvat proposal does not answer those questions.<sup>36</sup>

To provide SAF-T quality real-time transactional data, RTvat would need to develop a secure data recovery system, and put this system in place in the estimated 35 million businesses in the European Union.<sup>37</sup> There are systems available today that can do this – gather data for all taxable transactions, store it securely on site, encrypt

to the principle that VAT depends on the nature of the supply, not on the status of the customer. In addition, there is the possibility of fraudulent exemption certificates, and there is no enforcement mechanism in the government holding taxpayer's funds (even for a short period of time).

See: Richard T. Ainsworth, "Tackling VAT Fraud: 13 Ways Forward", 45 *Tax Notes Int'l* 1205, 1208 of 26 March, 2007.

32. PricewaterhouseCoopers estimates that MTIC/MTEC fraud (which RTvat handles very well) is the third most significant contributor to the VAT gap. It falls just behind non-compliance (including suppression fraud) and VAT avoidance schemes. See PricewaterhouseCoopers, "Study on the feasibility of alternative methods for improving and simplifying the collection of VAT through the means of modern technologies and/or financial intermediaries", Final Report 129 of 20 September 2010 (indicating that the contributors to the VAT gap are: non-compliance, including suppression fraud, (24-38%); VAT avoidance schemes (24-28%); MTIC/MTEC fraud (17-26%); threshold fraud (4-5%); and other components of the VAT gap, including insolvencies (3-24%), available at: [http://ec.europa.eu/taxation\\_customs/resources/documents/common/consultations/tax/future\\_vat/vat-study\\_en.pdf](http://ec.europa.eu/taxation_customs/resources/documents/common/consultations/tax/future_vat/vat-study_en.pdf).
33. Suppression fraud is based on manipulation of sales data by means of zappers and phantomware applications installed in electronic cash registers.
34. TASS reportedly does more than settle VAT liabilities – it provides the tax authorities with a state-of-the-art fraud analysis tool.

Tax authorities will be provided with a sophisticated Fraud Analysis and Security Tool (FAST), similar to those used by card association member banks, to identify unusual transactions. Those traders which are identified by the system as "suspicious" can be flagged for further investigation and the refund of input VAT suspended until queries are resolved. ... The system provides the merchant with applicable rates of VAT for all goods and services across the EU, enabling a quick and easy submission of this information with every settlement. ... The tax authorities have "real time" reports identifying all intra-EU transactions, and showing the relevant VAT number of both parties.

See "RTvat: An Introduction", note 25, pp. 7 and 8.

35. OECD, *Guidance Note for the Standard Audit File – Tax* (May 2005) available at: [http://www.oecd.org/LongAbstract/0,3425,en\\_2649\\_33749\\_34910278\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/LongAbstract/0,3425,en_2649_33749_34910278_1_1_1_1,00.html).
36. According to Chris Williams in "RTvat: A Real-Time Solution for Improving the EU VAT System, Removing Intra-EU Carousel Fraud and Reducing other VAT Losses" of 2 August 2009, pp. 10 and 11, TASS contains an XML Matrix. FAST will work on data stored in the XML Matrix within TASS to uncover potential frauds and report them to the tax authorities.

The XML Matrix sitting at the heart of the real-time solution will track all transaction information for business-to-business, business-to-consumer domestic and cross-border transactions, and will disseminate all information between EU tax authorities within a daily time frame. It will also provide access to product and service codes and applicable VAT rates across all Member States. Individual tax authorities, through the individual risk analysis tools associated with their own servers, will have the facility to control the extent and the granularity of fraud checking within their own Member State and the ability to communicate fraud status to other tax authorities. Each tax authority will be able to tailor the fraud scoring thresholds and the blocking or delaying of reclaims according to their own criteria.

See "RTvat: An Introduction", see note 25, p. 15.

37. PricewaterhouseCoopers, *Improving and simplifying the collection of VAT*, see note 32, p. 115, estimated that there were 34,895,924 registered businesses in the European Union in 2009.

and digitally sign it, and then transmit it to a remote audit location.<sup>38</sup> Data transmission can be of SAF-T quality<sup>39</sup> and in real time – transmitted daily or immediately after a transaction is completed.<sup>40</sup> Developed to secure electronic cash registers (ECRs) against suppression fraud, and then securely transmit critical tax data to authorities for remote audit, this technology can be applied (B2B as well as B2C) to give governments the real-time database they need to close the VAT gap in certain areas outside missing-trader fraud.

### 2.3. D-VAT certification

The use of certified tax software and certified service providers can limit the risk of specific types of fraud and other irregularities, and it can provide certainty to honest businesses engaged in domestic and cross-border transactions.

Certified software is currently being used on a voluntary basis in the US retail sales tax by 23 states<sup>41</sup> under the Streamlined Sales and Use Tax Agreement (SSUTA).<sup>42</sup> The same certification mechanisms could be applied to make VAT systems more robust.

The SSUTA has authorized three types of certified tax systems:

- certification of software systems developed by third parties, which are used internally in a business' accounting system;
- certification of a business' own tax accounting system developed internally; and
- certification of third parties as service providers.

The dominant approach in the United States is the use of certified service providers (CSPs). These CSPs commonly provide their customers' tax returns, guarantee and settle their customers' tax liabilities and provide other compliance services.

Under D-VAT certification, the tax authorities will develop a testing regime for the certification of enterprise-level transaction tax software.<sup>43</sup> To be certified, the software would need to be comprehensive and capable of:

- determining the correct tax rate for every transaction and calculating the VAT due;
- posting this amount on the related invoice;
- linking each input or output to the correct VAT return; and
- completing the VAT return accurately.

The system would also authorize the remission of taxes due. Many existing systems do this already; the difference is that they are not certified as being "accurate". In addition, the software will need to verify whether or not the companion system (the system used by the contract partner) is also certified.

Business use of certified software in the United States is voluntary. However, in some instances, notably when an enterprise is heavily engaged in transactions deemed inherently prone to missing-trader fraud, such as transfers of tradable CO<sub>2</sub> emission permits, supplies of cell phones or computer chips, a jurisdiction might make certified software a mandatory condition of doing business. In addition, in judicial proceedings, the authorities could seek

(as a fraud remedy) the mandatory adoption of certified software "going forward", based on proven instances of fraud in the past.<sup>44</sup>

- .....
38. Revenue Quebec has installed a Sales Recording Module (SRM) in restaurants, which preserves transaction data. An SRM costs approximately CAD 800 and is paid for and installed by the government. Revenue Quebec considered using the SRM in a remote audit capacity but decided at a policy level not to do so. Alagma Technologies manufactures the SRM for Revenue Quebec, see <http://www.allagma.com/products/srmmev-law-in-quebec/frequently-asked-questions-faq/>. Sweden has installed similar devices, which it has secured from several manufacturers. One company, BMC, has certified its eTAX system with the tax administration. Like Quebec, Sweden also does not use eTAX for remote auditing; see: <http://www.bmcinc.co.jp/product/control.html>. A device that would provide secure remote audit capacity based on the e-TAX design would cost less than USD 350 per unit. In 2011, several jurisdictions in the European Union will be adopting secure tax data preservation devices with remote audit capabilities. For example, the Slovenian Ministry of Finance indicates that it will install similar devices, but with remote audit capabilities, at EUR 20 per month per control module. Slovenia Ministry of Finance, *ZADEVA: Osnutek zakonskih podlag za uvedbo davčnih blagajn – predlog za obravnavo*, (Draft statutory bases for the introduction of tax cash registers), of 12 January 2011, Para. 3.3.
  39. Goran Todorov, R&D Manager at BMC-Balkan, personal e-mail communication of 26 January 2011; on file with author).
  40. Simultaneous transmission (transmitting to a remote location during the process of completing a B2B or B2C transaction) is problematical for businesses if it slows down the transaction itself.
  41. These 23 states are subdivided into two groups, the "full members" and "associate members". Full members are: Arkansas, Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Nebraska, Nevada, New Jersey, North Carolina, North Dakota, Oklahoma, Rhode Island, South Dakota, Vermont, Washington, West Virginia, Wisconsin and Wyoming. The associate members are: Ohio, Tennessee, and Utah, see <http://www.streamlined-salestax.org> (last visited 24 January 2009).
  42. The SSUTA was adopted on 12 November 2002, and amended on 19 November 2003 and further amended on 16 November 2004. The text of the agreement is available at <http://www.streamlinedsalestax.org> (providing for fully digital compliance with sales and use taxes through certified intermediaries and certified software solutions).
  43. The SSUTA certification process involves measuring software against three third-party standards; (1) the AICPA's SAS 94 [American Institute of Certified Public Accountants, Professional Standards, Vol. 1 AU Sec. 319 The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit, as amending SAS No. 55 Consideration of Internal Control in a Financial Statement Audit]; and (2) the US GAO Federal Information Systems Control Audit Manual [US Government Accounting Office, Accounting And Information Management Division, Federal Information Systems Control Audit Manual, (FISCAM) Vol. 1 (GAO-AIMD12.19.6) available at <http://www.gao.gov/special.pubs/ai12.19.6.pdf>]. In addition, software developers must comply with (3) ISO Number 17799 [International Organization For Standardization, Iso 17799: Information Technology, Security Techniques, Code For Information Security Management (ISO/IEC 17799:2005)]. A discussion of similar standards for certification and accreditation of software can be found in the recent OECD materials [*Electronic Commerce: Facilitating Collection of Consumption Taxes on Business-to-Consumer Cross-Border E-Commerce Transactions*, OECD (11 February 2005) at 9 and 17-18 available at <http://www.oecd.org>. Indicating that, "... a global intermediary may be based in one country and would undertake intermediary activities in as many countries as suppliers are required to collect and remit consumption taxes on behalf of e-commerce suppliers. In cases where satisfactory levels of approval or financial security are evident, countries could be more relaxed ...". The OECD discusses a range of government "approvals" for tax accounting software. At one extreme is "accreditation", an approval process that functions simply as a mechanism to "formally identify" software that meets certain criteria of acceptability. At the other extreme is "certification", an approval process that designates software as "an officially authorized mechanism to perform specified functions."].
  44. This was the approach adopted by Judge Lise Gaboury of the Court of Quebec in the fraud case against the 28-restaurant chain Casa Grecque. In this instance, the fraud involved installing an automated sales skimming programme called a Sales Zapper in the point of sale system (the networked electronic cash register). In the Budget Speech of 23 March 2006, the Minister of Revenue had announced the adoption of an automated system (*module d'enregistrement des vents*), which would be voluntary until 2011. Judge Gaboury noted that the system was expected to be available by 1 October 2008 and required all of the Casa Grecque restaurants

Similar to VLN, D-VAT certification, which covers both cross-border and domestic transactions, does not affect the destination principle of the current EU VAT system. Theoretically, D-VAT certification will allow businesses to zero rate intra-Community supplies of goods if the customer also uses certified software, which means that the customer's software will ensure that the accompanying intra-Community acquisition of the goods will be subject to VAT in the Member State of destination. However, under current EU VAT law, there is not an immediate and direct link between the application of the zero rate to intra-Community supplies and taxation of the accompanying acquisitions in the Member State of destination. Intra-Community supplies are only zero rated if the supplier can show that the goods have physically left the Member State of departure of the goods. The circumstance that the customer has accounted for VAT on the acquisition in the Member State of destination of the goods is not relevant in that respect.<sup>45</sup>

D-VAT certification is also unable to protect honest businesses against getting involved in missing-trader fraud. The fact that a customer uses certified tax software does not prevent its fraudulent supplier from going missing with the VAT, unless the supplier also uses certified tax software, in combination with a certified service provider, who guarantees remittance of the supplier's VAT liability. It is, however, extremely unlikely that fraudulent traders will make use of the services of CSPs. Moreover, the more the tax authorities know about the prices of specific goods at preceding and subsequent stages of the process of distribution, the easier it will be for them to spot a dip in the price and prove that an "innocent" trader should have realized that it was involved in a fraudulent transaction, which has the effect that the trader loses the right to deduct input VAT, even though it may use certified tax software or even a CSP.

The use of certified tax software is obviously ineffective for preventing missing-trader fraud and it is absolutely unrealistic to require 35 million businesses in the European Union, including small and medium-sized businesses) to make use of the services of CSPs. Compulsory use of CSPs in fraud-prone sectors is hardly a solution because missing-trader fraud can easily move to another sector.

### 3. Conclusions

Since it has a broad base and is imposed at high rates, VAT has always been vulnerable to missing-trader fraud. The earliest versions of fraud in the European Union concerned smuggling gold across the Luxembourg border, selling it (with VAT) in another Member State, and then disappearing.<sup>46</sup> In response, Member States may apply the reverse charge mechanism to those supplies, from 1 January 2000.<sup>47</sup>

We are a long way from smuggling gold when we consider missing-trader fraud in VoIP services and digitized CO<sub>2</sub> permits. Technology allows the fraudsters to move faster, and the size of the fraud

increases without limit. Enforcement needs to move just as fast.

Of the options considered above, VLN may offer a solution for missing-trader fraud in specific sectors but it cannot cover the entire economy of the European Union. D-VAT certification has undoubtedly a positive effect on VAT compliance but it does not resolve the problem of missing-trader fraud. In addition, the use of CSPs will be too expensive, in particular for small and medium-sized businesses.

The only solution that is actually capable of preventing missing-trader fraud and also limits several other forms of fraud, such as suppression fraud, is RTvat. It retains all safety mechanisms of a true VAT system and, at the same time, prevents the collection risk for the tax authorities. RTvat is based on the principle that transactions are paid for through banks, which is already the common method of payment for B2B transactions and, increasingly, also for B2C transactions (final consumers increasingly pay with plastic money). It requires a shift of the time on which VAT liabilities arise and input tax can be deducted, but that amendment should have a positive effect on the economy as a whole.

None of these solutions, including RTvat's TASS, FAST, and the XML Matrix, appears to be able to fully close the VAT gap and to prevent all possible types of fraud and VAT avoidance. Traditional audits will continue to be necessary in the future to combat sophisticated VAT avoidance schemes. However, the more robust the basic VAT system is, the more time inspectors and auditors can devote to closing other leaks in the VAT system. RTvat is by far the most promising and practical solution for a robust VAT system. However, the technical specifications of the system need further attention.

to adopt it at this time as a condition of remaining in business. Revenue Quebec, *Des restaurants de la chaîne Casa Grecque coupables de fraude fiscale* (in French only) available at: [http://www.revenu.gouv.qc.ca/eng/ministere/centre\\_information/communiqués/ev-fisc/2006/10juillet.asp](http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiqués/ev-fisc/2006/10juillet.asp)

45. In its judgment of 27 September 2007 in *Twoh International BV v. Staatssecretaris van Financiën*, Case C-184/05, [ECR] I-7897, the ECJ observed that it should be added that, even if the tax authorities of the dispatching Member State did obtain information from the destination Member State that the buyer had submitted a declaration to the tax authorities of that latter State that there was intra-Community acquisition, such a declaration does not constitute decisive proof capable of establishing that the goods actually left the territory of the dispatching Member State.
46. A.A. Aronowitz, D.C.G. Laagland and G. Paulides, *Value-added Tax Fraud in the European Union 75-76* (1999) (discussing how gold was smuggled from Luxembourg where the VAT rate was 0% into other Member States where it could be sold with VAT). Awareness of the gold-smuggling problem eventually resulted in the adoption of a special regime for gold. See: UK Parliament, Select Committee on European Union, Twentieth Report, *Chapter 2: Tackling MTIC Fraud: Actions to Date*, Sec. 38 (indicating that a "Special Accounting System for Gold" was introduced in April 1993 to combat VAT fraud in that market), available at: <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldauc/101/10105.htm>.
47. Member States have the power to apply the reverse charge mechanism to domestic supplies of gold material or semi-manufactured products of a purity of 325 thousandths or greater and to supplies of investment gold under Art. 26b(F) of the former Sixth Directive, as amended by Art. 1 of Directive 98/80/EC and under Art. 198 of the current VAT Directive.