8-26-2011

Technology Solves MTIC - VLN, RTvat, D-VAT Certification

Richard Thompson Ainsworth

BU School of Law

TECHNOLOGY SOLVES MTIC – VLN, RTVAT, D-VAT CERTIFICATION

Boston University School of Law Working Paper No. 11-07
(February 14, 2011)

Richard T. Ainsworth

TECHNOLOGY SOLVES MTIC – VLN, RTvat, D-VAT certification

Richard T. Ainsworth

Technology solves missing trader intra-community (MTIC) fraud.[1] This should come as no surprise. MTIC is technology-intensive fraud – its solution should also be technology-intensive.

In the early 2000's when MTIC was all about cell phones and computer chips, newspaper reporters visited fraudsters and got lessons on how easy it was to turn the carousel[2] – provided you had a laptop.[3] At this time MTIC was in the process of morphing from a fraud that was primarily concern with the physical movement of goods across community borders to a fraud that was primarily a function of technology. Goods would stay in customs warehouses[4] – the fraud would be carried out on laptops.

By 2006 MTIC had morphed again.[5] Now MTIC was targeting services (CO2 permits and VoIP). Once again (after it was uncovered) newspapers carried stories about how it was even easier to carry out this variant of MTIC. In these cases the supply itself, the CO2 permit or VoIP minutes (not just its movement) was digital. Fraudsters on the BlueNext exchange reportedly worked their frauds from laptops in the comfort of Parisian cafés.[6] With the attack on services MTIC also became an "extra-community" fraud (MTEC).[7]

[1] MTIC is getting to be an out-dated term. Now that missing trader fraud has move into services it is no longer confined to intra-community trade. Norway is just as concerned about missing CO2 traders in Nord Pool, as are the French with these same traders on the BlueNext, and the Italians on the GME. 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] MTIC fraud is also known as carousel fraud, because the same goods go around in circles – trading many times among the same parties.

[3] 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

> 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."

[4] *But see*: Teleos, Plc and Others v. HMRC, C-409/04 (indicating that goods must physically be exported to qualify for zero-rating, and not remain in a customs warehouse).

[5] 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 (May 31, 2010). CO2 trade began on January 1, 2005. In December of 2009 Europol said it had been tracking this mutation for 18 months, so this strain of MTIC dates back at least to 2007. *See*: Richard T. Ainsworth, *CO2 MTIC Fraud – Technologically Exploiting the EU VAT (Again)*, 57 TAX NOTES INT'L 357 (January 25, 20100.

[6] Aline Robert, *La fraude a la TVA du CO2 se revele gigantesque,* La Tribune 22 (Dec. 16, 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 tones of CO2 while quietly installed in their Parisian cafes. Using temporary internet addresses on

Enforcement also shifted. Tax authorities began following the funds. The UK, for example, discovered that most of the money it was chasing had transferred among accounts at the same offshore bank, First Curacao International Bank (FCIB). FCIB was shut down.[8]

Fraudsters responded, and predictably the response was digital. Internet payment platforms[9] 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.

> sites like Yahoo! or Gmail also makes it easier for crooks. The cases reveal a crying absence of regulation in the CO2 market.

[7] Richard T. Ainsworth, *VAT Fraud: The Tradable Service Problem*, 61 Tax Notes Int'l 217 (January 17, 2011) (discussing the morphing of MTIC into MTEC and introducing the expression).

[8] Ian Cobain & 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 (September 21, 2006); First Curacao International Bank, Press Release 06-013, *First Curacao International Bank N.V. Subject to the Emergency Measure* (October 11, 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

[9] The press is ahead of tax enforcement with respect to online payment platforms. In CO2 MTIC/MTEC these platforms register on an exchange (recently the Danish exchange has been popular) hold a single large account with a traditional bank, but take deposits and make transfers for traders (normally for €500 when a traditional bank would charge €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 intenet when they become part of an inquiry. See for example: First Bancorp Ltd.

> First Bancorp Limited 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 ion the Danish exchange [Europol Press Release, *Carbon Credit fraud causes more than 5 billion euros damage for European Taxpayer* (Dec. 9, 2009) a*vailable at*: http://www.europol.europa.eu/index.asp?page=news&news=pr091209.htm.].

Experimenting with this process Bo Elkjaer and John Mynderup (journalist with Ekstra Bladet) made contact with the Director of Swefin [http://swefin-online.com/?page=tac], Donald Garbo. [Bo Elkjaer & John Mynderup, *Anders Garbro: Jeg svindler ikke med CO2* (*Donald Garbro: I do not tamper with CO2*), Ekstra Bladet (December 3, 2010) [in Danish, translation on file with author]. Garbro initially acknowledges 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 on Friday, December 3, called another Director of the company, Kashif Ghaus Qadri, who had lived in Ishoej, Denmark, but recently moved to Dubai, UAE.

> On the night of Friday [December 3, 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 CO2 allowances in the scandal that has hit the Danish quota registry.

Bo Elkjaer & John Mynderup, *Dansk Kvotesvindler I Luksus I Dubai,* (*Danish Quota Fraudster* [*Living in*] *Luxury in Dubai*), Ekstra Bladet (December 6, 2010) [in Danish, translation on file with author]. Unfortunately, closing an internet payment platform does not have a significant impact on CO2 fraud as there are hundreds of similar platforms, platforms constructed on top of platforms, with more platforms ready in the wings to move in, assume control of funds and continue business as usual. This is much easier for the fraudsters than closing an offshore bank, like FCIB.

MTIC/MTEC fraud was now fully digitized (the supply, the movement of the supply, and the funding). The consequences should be clear. MTIC/MTEC 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 counter-measure for this fraud.

We have known the details of the three major technology-intensive proposals for solving MTIC/MTEC since 2007: the VAT locator number (VLN);[10] real time VAT (RTvat),[11] and certified tax software (D-VAT).[12] This paper endeavors to contribute to the debate that the Commission has opened on this topic with its recent Green Paper[13] by comparing and contrasting these proposals.

> The Green Paper on the future of VAT launches a wide consultation process with all stakeholders on the current VAT system and the possible ways to strengthening 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.[14]

TECHNOLOGY SOLUTIONS

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

Both the VLN and RTvat are mandatory systems. The VLN focuses on securing every supply, whereas the RTvat focuses on securing every payment. D-VAT certification differs in both respects. It can be adopted on a voluntary basis (per taxpayer) and achieves a secure remission of VAT through trusted third parties. These third parties are providers that stand between the taxpayer and the tax administration, complete all filings, and remit payments – guaranteeing the accuracy of the return and the satisfaction of the tax due.

[10] HOUSE OF LORDS, EUROPEAN UNION COMMITTEE, STOPPING THE CAROUSEL: MISSING TRADER FRAUD IN THE EU (REPORT WITH EVIDENCE) HL Paper 101(May 25, 2007) at 78-82; Michael Cheetham, *For who so firm that cannot be seduced?* (2007 powerpoint presentation) at 20-23; 29-34 (on file with author).

[11] Charles Jennings, *The EU VAT System – Time for a New Approach?* INT. VAT MONITOR 257 (July/ August 2010); further details are available at: http://www.rtvat.eu/.

[12] *See*: Charlene-Adline Herbain, *VAT Fraud on Carbon Allowances,* TAX PLANNING INT. – INDIRECT TAXES (Sept. 2009) 4 (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 (Aug. 31, 2009) (setting out a targeted solution to MTIC in the CO2 market); Richard T. Ainsworth, *Car Flipping in the UK The VAT Fraud Marketplace and Certified Solutions,* 47 TAX NOTES INT'L. 1157 (Sept. 24, 2007) (assessing the car-flipping VAT fraud in the UK 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 (Apr. 16, 2007) (comparing car-flipping fraud in Canada with MTIC fraud in the UK and proposing a certified software solution); Richard T. Ainsworth, *Tackling VAT Fraud: 13 Ways Forward*, 45 TAX NOTES INT'L. 1205 (Mar. 26, 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 (May 1, 2006) (setting out a fully digital solution for MTIC fraud).

[13] European Commission, *Green Paper: On the Future of VAT – Towards a simpler, more robust and efficient VAT system*, COM(2010) 695/4.

[14] EU Commission, *Questions and Answers: Value Added Tax (VAT)* (December 1, 2010) *available at*: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/633&format=HTML&aged=0&language=EN&guiLanguage=en

There is a considerable amount of central control under both 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 transaction is completely and accurately reported because the systems performing these operations are certified and guaranteed.

Finally, both the VLN and D-VAT certification go to great lengths to avoid making fundamental changes in the way the EU VAT currently operates (the VLN perhaps even more than D-VAT certification). In addition, both VLN and D-VAT certification can be adopted one Member State at a time. The RTvat proposal differs on both accounts. It fundamentally changes the EU VAT into an origin system, and requires adoption by all Member States to be fully effective.

VLN

The VAT Locator Number system is the simplest of the three technology solutions. It is the least disruptive to the current VAT system. It was formulated and proposed by Dr. Michael Cheetham at the House of Lords hearings, May 25, 2007.[15] The VLN solution is very targeted. It is *only* looking at solving MTIC/ MTEC fraud. It can be adopted by a single Member State to prevent MTIC/ MTEC losses without requiring the cooperation of any other jurisdiction.

The most significant policy change made by the VLN proposal is the denial of a buyer's input credit if VAT is paid on an invoice with an invalid VLN (or no VLN at all). The most significant procedural change is that businesses will be required to secure a valid VLN, and attach it to an invoice (when selling supplies).

In most cases both sides of this compliance measure will be fully automated. Accountancy software platforms will make automated *requests* for VLNs 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 manufacture through to final consumption. A back-up system where VLNs are secured through an internet web site or a call center will be available.[16]

The VLN system requires the seller with each transaction to secure and print on the invoice an encrypted VLN. This number will be unique to a specific transaction (based on the essential data elements of the invoice, and prior related VLNs 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.[17] The advantage of a bar code and optical

[15] HOUSE OF LORDS, *supra*, note 10.

[16] Dr. Michaels Cheetham, *Personal e-mail communication* (April 25, 2010) (on file with author).

[17] A similar bar code is added to each cash register receipt issued by Quebec restaurants under their 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 an auditor in a thirty-minute visit, observes that customers are receiving receipts, and then quickly verifies (with the scanner) that the receipts being issued are recorded in the SRM. Full inspections can follow in cases of irregularities. Gilles Bernard, *Solutions for the Under-reporting of income in the Restaurant*

reader capabilities is that a trader can quickly scan the VLN bar code into a national database to verify the VLN.

A similar fraud prevention system is in place in Brazil, where it has proven to be highly reliable. In Brazil invoices receive a digital bar code at internal (inter-state) borders from a federal computer feed. The bar code validates the invoice and the physical transit of the goods.[18]

Example. An example of how the VLN works is helpful. If business B-1 in France sells goods or tradable services to business B-2 in the UK, B-1 will zero rate the transaction out of France (or in the case of services the French VAT will not apply because the place of supply will be the UK). B-2 will request a VLN (for performing a reverse charge) from HMRC's central computer system. The number returned will be VLN-1.

The request made by B-2 will include the essential elements of the invoice received from France. HMRC will perform a risk assessment (based on B-2's past compliance history, the size of the present transaction, and some judgment as to whether or not this is a "normal" transaction for this business). If B-2 is deemed by HMRC to be a low risk importer (not likely to "go missing"), then VLN-1 will issue.[19]

B-2 will then perform the standard reverse charge.

VLN-1 is an encrypted identifier. It includes all the essential attributes of the B-1/ B-2 transaction. It will be integrated into all subsequent VLNs in this chain. When B-2 seeks to make an onward sale (to B-3) of all or some of these supplies, B-2 will request a new VLN for the onward invoice. As before, B-2 will submit (a) all the essential attributes of the onward

Sector, Federation of Tax Administrators Annual Conference, Denver Colorado (June 2, 2009) powerpoint slides at 15-17 (on file with author).

[18] A number of Brazilian states and the federal government signed an agreement on September 30, 2005 to create (1) the "e-invoice" ("Nota Fiscal Eletrônica") and (2) the "auxiliary document of the e-invoice" ("Documento Auxiliar da Nota Fiscal Eletrônica"). *AJUSTE SINIEF N.º 07 DE 30 DE SETEMBRO DE 2005*) *available at*: http://www.sef.rj.gov.br/legislacao/tributaria/convenios_ajustes_protocolos/confaz/ajustes/2005/aj05007.shtml. On December 20, 2005, through the ATO COTEPE/ICMS N.º 72 DE 20 DE DEZEMBRO DE 2005 http://www.sef.rj.gov.br/legislacao/tributaria/convenios_ajustes_protocolos/confaz/pareceres_ecf/2005/ato072_05.shtml the structure of the e-invoice was established and testing was initiated with nineteen companies and those companies and six states. The program has been deemed a success and has been extended.

[19] In instances where an adequate risk assessment cannot be performed (for example where the importing UK business is newly formed) a VLN will not issue. Under the VLN system this business will be required to perform a reverse charge with a direct payment of VAT to the Treasury. In this respect RTvat follows solutions that Dr. Cheetham presented in the House of Lords, *supra* note 10, at 89-90:

> Can I just say something extra which is important about the VAT logging system? Because of the FTI case [*Federation of Technological Industries and 53 others*, C-384/04] and their success in the European Court of Justice, one of the things the European Court said they could do is require a security guarantee. That means you can ask a company to deposit VAT or its equivalent. With my VAT logging system what you do is when the system pops up on the Customs computer they go to the company and say, "OK, we require that VAT be deposited with us – first deal." Now, missing traders usually have to make a loss and, therefore, they would not be able to deposit that number so you turn off the logging system and that company can no longer trade. So, you run that system, you make them deposit the VAT, and under the security guarantee rules the missing trade will not be able to operate and it will eliminate [MTIC].

invoice, and (b) a copy of VLN-1 (which it received from HMRC after the importation from France). If this request passes HMRC risk assessment a new number will issue (VLN-2).

B-2 will place VLN-2 on the onward invoice.[20] When B-3 receives the invoice from B-2 it should not pay VAT until it verifies the validity of VLN-2. If it pays without checking, then B-3 will be at risk of being denied a deduction for VAT paid if (a) the VLN on the invoice is invalid or if (b) there is no VLN on the invoice at all.

Because VLN-2 includes not only data from the B-2/ B-3 transaction, but also data from the B-1/ B-2 transaction HMRC will be able to reconstruct the full commercial chain. Because B-3 will be on notice that its deduction is in 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 partners in the chain).[21] If VLN-2 is confirmed by HMRC as a valid number, B-3 will be assured that it can deduct the VAT it has paid. If there is any question on the part of HMRC that the transaction is suspect, HMRC can stop VAT from being paid, by rejecting the VLN request. This will not necessarily stop the commercial transaction, but buyer and seller would be on notice that some other arrangement for payment of the VAT is needed.

The automatic response of the *next trader in line* when there is a VLN irregularity is to pay the seller for the supply, but pay all of the VAT to the tax authority.[22] The VLN will allow this payment, and the tax authority will send a receipt to both parties. This is probably the only action that will allow the buyer to quickly secure a follow-on VLN for re-selling the supplies. Because no deductible VAT is ever paid to a business that sells without a valid VLN MTIC/ MTEC fraud is eliminated.

RTvat

In some respects the RTvat is born of the same insights as the VLN. The application is different however. The VLN is applied to the supply side – the RTvat is applied to the payment side of taxable transactions.

[20] In cases where the onward sale is comprised of multiple supplies two avenues are available: either separate invoices are issued for each supply (each with a discrete VLN), or an aggregate invoice could issue (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 (January 23, 2011) (on file with author).

[21] Due diligence requirements are set out in *Axel Kittel v. Belgium*, C-439/04 (July 6, 2006). 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.

[22] This is in fact the operating principle of the RTvat. However, rather than being the solution to a problem caused by an invalid VLN, under the RTvat splitting the payment so that the base charge goes to the supplier and the VAT is directly remitted to the tax authorities is the way *all* transactions are carried out.

Both VLN and the RTvat use central (government) computers to tract all transactions, but where the VLN digitally tags each supply, the RTvat digitally sequesters each VAT payment. Unlike the VLN that penalizes traders that pay VAT over an invalid VLN, the RTvat simply eliminates the possibility of making this payment.

The RTvat makes two significant structural changes to the VAT, along with a dramatic procedural adjustment. First, it changes the VAT liability to the date the price is received (the right to deduct input tax shifts in tandem to the date the business pays its supplier).[23] Secondly, the RTvat is an origin-based (not a destination-base) tax system.

> The VAT liability in respect of intra-Community supplies of goods and services is based on the origin system, which is still envisaged as the "definitive system" under Art 402 of the VAT Directive.[24]

However, it is a procedural change that is the most striking attribute of the RTvat.[25] Under RTvat suppliers only receive the tax-exclusive price for their supplies. The VAT element is split off from the buyer's payment and is separately (electronically) remitted to the tax authorities from the buyer's bank account. The RTvat works well with payments by cash or check, but there is a distinct preference for electronic funds transfer (EFT). With ETF the refund of deductible VAT is possible the same day the VAT is received by the tax authority.[26]

RTvat borrows the payment system of the credit card industry and applies it to VAT collection[27] – a dedicated B2B debit card is envisioned to facilitate fund transfers.[28] A network

[23] The information brochure *RTvat: An Introduction to a Real-time Solution for Improving the EU VAT System* 5 (March 2009) (on file with author) indicates that the RTvat is:

> **A settlement-based system:**
> Changes the payment and refund of due VAT from an invoiced based system with delayed periodic declarations to a system based on settlement at the point at which funds are paid.

[24] Jennings, *supra* note 11, at 257.

[25] The RTvat also includes "a sophisticated fraud analysis tool, based on analytical applications currently used in the credit card and financial services arenas," although it is unclear what value this adds to the proposal.

[26] As a settlement-based system cash and check payments delay the refund mechanism, because they delay the VAT payment to the tax authority.

> 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) I banked. The VAT on cash transactions is captured when the supplier transfers his takings to his bank account; …

Jennings, *supra* note 11, at 258.

[27] A number of jurisdictions outside the EU have rules very similar to the 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. [VATA Art. 63, Regulations 118 – 120 (Equ.)] Colombia has a similar law, but the amount remitted is 50% of the VAT on all payments made with credit/debit cards. [VATA Art. 437-1 (Col.)]. 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 credit card companies.

[28] Jennings, *supra* note 11, 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.

of twenty-seven identical linked servers (one in each Member State) will act as communications and fund transfer centers. Each Member State will own and operate its own server and all domestic transactions will be processed through it. The server separates and transmits the VAT element on each transaction, and transmits the funds to the tax authorities.

MTIC/ MTEC fraud is impossible. No trader ever holds the VAT for the government. It is impossible to go "missing" with the VAT in hand under the RTvat.

If the RTvat stopped at this point the proposal would be striking for its simplicity, originality and workability.[29] However, RTvat goes further. It endeavors to solve far more than the MTIC/ MTEC slice of the VAT Gap, and in doing so the RTvat proposal becomes confusing. In short, the RTvat overreaches. It gets caught in data collection and security issues that it is not able to address.

PricewaterhousCoopers estimates that MTIC/ MTEC fraud (which the RTvat handles very well) is the third most significant contributor to the VAT Gap. It falls just behind (a) non-compliance (including suppression fraud) and (b) VAT avoidance schemes.[30] Both of these schemes are highly vulnerable to data-mining and sophisticated risk analysis measures, but these measures require comprehensive (real-time) databases to produce good results. RTvat attempts to solve these frauds, but cannot.

RTvat does not gather for itself, nor does it transmit to tax authorities detailed real-time, invoice-level transaction data of a type one would expect to receive under the OECD's Standard Audit File – Tax[31] (SAF-T) format. The reason it does not is simple – RTvat is a payment-side, not a transaction-side solution. RTvat does not collect, organize or process *invoice data* elements; RTvat collects, remits and facilitates *VAT payments and refunds*.

RTvat's confusion. The confusion with RTvat begins when the server network is examined. RTvat establishes a computer network in the 27 Member States primarily to facilitate VAT transfers, but it embeds within this network the Tax Authority Settlement System (TASS).

[29] It is important to note however, that much of what the RTvat does has been considered in the *Mittler Model* which 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 (English and German). The central difference between the RTvat and the Mittler Model is that the Mittler Model works with exemption certificates instead of cash. There is no banking system involvement under the Mittler Model. The Mittler Model is therefore much less expensive to operate and is more workable. There is the possibility of fraudulent exemption certificates under the Mittle Model, 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 (Mar. 26, 2007).

[30] PricewatherhouseCoopers, 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 (September 20, 2010) (indicating that the contributors to the VAT gap are: (a) non-compliance (including suppression fraud) 24-38%; (b) VAT avoidance schemes 24-28%; (c) MTIC/ MTEC fraud 17-26%; (d) threshold fraud 4-5%; and (e) 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

[31] Tax-critical elements of the invoice are set out in 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

TASS reportedly does more than *settle* VAT liability – it provides tax authorities with state of the art fraud analysis tools.

> 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 trades 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.[32]

There are too many unanswered questions about the scope and content of the data in TASS. Specifying the *VAT ID numbers* of both parties and *identifying* all intra-EU transactions is a long way from SAF-T data. There is nothing to suggest in any RTvat documentation that it is even attempting to collect SAF-T data.

If however, RTvat does gather SAF-T quality data from all EU businesses it faces two data security issues that it also does not address: (a) it will need to guarantee that its data has not been tampered with before it arrives,[33] and (b) it will need to protect the data it has from external attack while it is retained and while it is transmitted (cyber criminals are all too anxious to learn anything they can about the real-time commercial activities of competitors).

The RTvat proposal has more detail, but it is not helpful. TASS, we are told, contains an XML Matrix.[34] Documents suggest that 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 Martix 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.[35]

[32] *RTvat: An Introduction*, *supra* note 23, at 7 & 8.
[33] One of the frauds RTvat hopes to deal with is suppression fraud. This is a fraud that is directly involved with the manipulation of sales data to avoid tax.
[34] Chris Wiliams, *RTvat: A real-time Solution for Improving the EU VAT System, Removing Intra-EU Carousel Fraud and Reducing other VAT Losses*, (August 2, 2009) at 10 & 11
[35] *RTvat: An Introduction*, *supra* note 23, at 15.

The question this discussion raises is – if tax authorities already have *risk analysis tools* adequate to the task of detecting fraud, and of doing so in a granular a manner, then what the Member States really need is real-time SAF-T quality data. Where can they get it?

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 (taxable persons) in the EU.[36] There are systems available today that can do this – gather data for all taxable transactions, store it securely on site, encrypt and digitally sign it, and then transmit it to a remote audit location.[37] Data transmission can be of SAF-T quality[38] and in real-time – transmitted daily or immediately after a transaction is completed.[39] Developed to secure electronic cash registers (ECR's) against suppression frauds, 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 areas outside MTIC/ MTEC fraud.

RTvat does not do this. As a result, TASS, FAST, and the XML Matrix are not enough to close the VAT Gap. RTvat does not have SAF-T quality data to work with, and cannot get it. RTvat can solve MTIC/ MTEC fraud, and can significantly diminish VAT losses from insolvencies, but it is helpless in the face of non-compliance (including suppression fraud) and sophisticated VAT avoidance schemes. The weakness in the RTvat comes from its overreaching, not from reaching what it can.

[36] PricewaterhouseCoopers, *Improving and simplifying the collection of VAT, supra* note 30, at 115 (estimating as of 2009 that there are 34,895,924 taxpayers in the EU).

[37] Revenue Quebec has installed a Sales Recording Module (SRM) in restaurants that preserves transaction data. An SRM costs approximately $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 audit, *see*: http://www.bmcinc.co.jp/product/control.html. A devise that would provide secure remote audit capacity based on the e-TAX design would cost less than $350 per unit. During 2011 several jurisdictions in the EU will be adopting secure tax data preservation devices with remote audit capabilities. For example the Slovenian Ministry of Finance indicates that they will install similar devices, but with remote audit capabilities:

> **3.3. Data transmission services from the control module to a central location TARS**
>
> Data transmission services, depending on the type of control module, transporting data over a mobile technology service providers GPRS, UMTS, MMS or via the Internet. Cost of GPRS solution consists of the cost of purchasing a SIM card and services, and costs by the quantity of data transferred. Estimated expense would be about 20 EUR / month / per control module. Of course, we anticipate that competition among service providers can provide significantly lower costs. Cost solutions that would make use of the Internet network are about the same, 20 EUR / month / control module, of course, assuming that it applies only to one network connection to Internet, otherwise the cost would be proportional to the number of connections in use.

Slovenia Ministry of Finance, *ZADEVA: Osnutek zakonskih podlag za uvedbo davc□nih blagajn – predlog za obravnavo* (*SUBJECT: Draft statutory bases for the introduction of fiscal cash registers*) (January 12, 2011) at 3.3

[38] Goran Todorov, R&D Manager at BMC-Balkan, personal e-mail communication (January 26, 2011) (on file with author).

[39] 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 sale itself.

D-VAT certification

Certified tax software can also solve MTIC/MTEC fraud. Certified software is currently being used in the US retail sales tax by 23 states[40] under the Streamlined Sales and Use Tax Agreement (SSUTA).[41] The same software mechanisms could be applied to the VAT to solve MTIC.

Similar to the VLN the D-VAT proposes to conditionally change the party required to collect and remit VAT. The condition revolves around whether buyer and seller use certified tax systems. If conditions are not met the seller will not be allowed to zero-rate the sale, and VAT will be due at origin. As with the VLN in most cases the VAT system under D-VAT certification will not be altered.

Certified tax software. Governments will develop a testing regime for the certification of enterprise-level transaction tax software.[42] To be certified the software would need to be comprehensive – capable of: (a) determining the correct tax rate for every transaction and calculate the VAT due, (b) posting this amount on the appropriate invoice, (c) linking each VAT input or output amount to the correct VAT return, and (d) completing the VAT return accurately. The system would also authorize the remission of taxes due. Many systems do this already, the

[40] These twenty-three states are divided into two groups, the full members, and the associate members. A full member state is a state that is in compliance with the Streamlined Sales and Use Tax Agreement through its laws, rules, regulations, and policies. Those states 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 (as of Oct. 1, 2009) and Wyoming. An associate member state is a State that has achieved substantial compliance with the terms of the Streamlined Sales and Use Tax Agreement taken as a whole, but not necessarily each provision, and there is an expectation that the state will achieve compliance by January 1, 2008. Those states are: Ohio, Tennessee, and Utah, *see* http://www.streamlinedsalestax.org (last visited Jan. 24, 2009).

[41] STREAMLINED SALES AND USE TAX AGREEMENT (adopted November 12, 2002, amended November 19, 2003 and further amended November 16, 2004) *available at* http://www.streamlinedsalestax.org [hereinafter SSUTA] (providing for fully digital compliance with sales and use taxes through certified intermediaries and certified software solutions).

[42] 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 § 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 [U.S. 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 O.E.C.D. materials [*Electronic Commerce: Facilitating Collection of Consumption Taxes on Business-to-Consumer Cross-Border E-Commerce Transactions,* O.E.C.D. (Feb. 11, 2005) at 9 & 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 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."].

difference is that they are not certified as accurate. In addition, the software will need to verify whether or not the companion system (the system used by the other trader) is also certified.

Business use of certified software is voluntary. In some instances however, notably when an enterprise is heavily engaged in transactions deemed inherently prone to missing trader fraud – like tradable emissions permits, cell phones, or computer chips – a jurisdiction might make certified software a mandatory condition of doing business. In addition, in judicial proceedings the government could seek (as a fraud remedy) the mandatory adoption of certified software "going forward," based on proven instances of fraud in the past.[43]

The SSUTA has authorized three types of certified software systems: certification of third-parties as service providers, certification of third-party software systems that are used internally in a taxpayer's accounting system, and certification of a taxpayer's own system developed internally. The dominant approach in the US is the certification of third-party providers. These third parties commonly provide tax return, money movement and other compliance services.

Four examples. Under D-VAT certification there are four permutations of possible results. They are set out below.

This solution is applicable globally, within an economic community, or by a single jurisdiction. Domestic transactions are not impacted. Assume a taxable transaction between two businesses (X and Y) where the parties are in different jurisdictions. The transactions involved could be the sale of *goods* or *tradable services*. Under standard EU VAT formulations, the transaction will be zero-rated leaving X's jurisdiction and subject to a reverse charge entering Y's jurisdiction.

If only Y is using a certified system, there should be no MTIC/MTEC problem with this transaction. A certified system will always perform a required reverse charge regardless of the certification of the other party's system. Y's VAT return will be properly prepared along with all related reports, and the funds will be properly remitted to the government. Problems arise when X is not using a certified system. The following four permutations summarizes these applications:

X certified; Y certified. If X and Y are both using certified systems the zero-rating and the reverse charge will be properly made, reported, and the VAT remitted to Y's government. This is true even if the transactions are occurring in suspect classes of supplies (cell phones, computer chips CO2 certificates or VoIP).

[43] This was the approach taken 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 program called a Sales Zapper in the point of sale system (the networked electronic cash register). In the Budget Speech of March 23, 2006 the Minister of Revenue had announced the adoption of an automated system [*module d'enregistrement des vents*] that would be voluntary until 2011. Judge Gaboury noted that the system was expected to be available by October 1, 2008 and required all of the Casa Grecque restaurants 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 fiscal* (in French only) *available at*: http://www.revenu.gouv.qc.ca/eng/ministere/centre_information/communiques/ev-fisc/2006/10juillet.asp

X not certified; Y certified. If X is not using a certified system and Y is using a certified system, then Y will reverse charge. The only question will be whether X's jurisdiction will allow a zero-rating in this case. Y's certified system will perform a reverse charge, but there needs to be a way for X's tax authority to confirm this directly.

If X was engaged in making supplies in a MTIC/MTEC prone industry, then the transaction might be questioned immediately. X's tax authority might consider it a "Community-duty" to deny zero-rating to X on the basis that it was not assured that the buyer in Y's jurisdiction was making a reverse charge.

The question would likely come down to whether or not X's jurisdiction is willing to accept Y's certification as proof that X had fulfilled a due diligence obligation to verify that Y was not participating in missing trader fraud. If so, then X should be allowed to zero-rate the sale even without a certified system.

There is a role for the EU Commission in this situation. The EU should validate national certifications and be able to assure all parties that X is working with a compliant system.

X certified; Y not certified. If X is using a certified system and Y is not, then X's system must be programmed to recognize this. X's system will not allow this transaction to be zero-rated. This would be particularly important if it occurred in a suspect class of supplies. X's system would impose the domestic tax.

Y would then be in a difficult situation. Potentially Y's purchases would be burdened with the VAT of two jurisdictions. Y would remain obligated to comply with the reverse charge in its own jurisdiction, and it would be paying VAT in X's jurisdiction on the same supply. Y would need to file for a refund in X's jurisdiction. In this situation Y would most likely either seek a domestic supplier (who would charge domestic VAT) or install its own certified system. This is the desired result in suspect supplies.

X not certified; Y not certified. If neither X nor Y uses a certified system, the risk of MTIC/MTEC is very high. In this situation there is no way for X's jurisdiction to be sure that the X-Y transactions are not part of MTIC/MTEC frauds. It might then condition the right of X to deduct VAT *paid* on suspect classes of supplies (cell phones, CO2 permits, VoIP) until it verified that VAT was *collected* on the reverse charge was performed.[44] This would essentially be a cash basis compliance regime. Once again, Y would be in a difficult position of being required to pay over VAT to X as well as reverse charging the supply.

In a certification regime that extends throughout a federal system (like the EU or Canada) notification that a system was certified would be automatic, handled through a secure on-line connections. A central government database would immediately verify the certification similar to the verification of a VAT ID and less burdensome than verifying the VLN on each transaction or the payments made under the RTvat.

[44] *Supra* note 19; *Federation of Technological Industries and 53 others*, C-384/04.

Dual checks and notifications would be expected. In the above examples it is equally important that X's system know about the status of Y's system, as it is that Y's system knows about X's status. There are a variety of ways this cross-verification can be accomplished, but the most proven and secure would be through the use of public key infrastructure (PKI).[45] X's system would access the public key associated with Y and use it to confirm the status of Y's system. With this knowledge, X would then draft an invoice with or without VAT and forward it to Y. If there were errors, Y's system would be checking the invoices received for the status of its suppliers before it paid over VAT.

In a sense this is simply automated due diligence. But in another sense, it is *certified* due diligence.

CONCLUSION

The VAT has always been vulnerable to missing trader frauds. At its core this fraud is smuggling. The earliest versions in the EU involved smuggling gold across the Luxembourg border, selling it (with VAT) in another Member State, and then disappearing.[46]

We are a long way from smuggling gold when we consider missing trader fraud in VoIP and digitized CO2 permits. Technology allows the fraudsters move faster, and the size of the fraud increases without limit. Enforcement needs to move just as fast.

Each of the solutions considered here, VLN, RTvat, and D-VAT certification, employ technology to *prevent* MTIC/MTEC rather than use technology to apprehend criminals after the fact. Both the VLN and RTvat have a strong government presence, whereas the D-VAT is a private sector solution. The VLN and RTvat are mandatory, whereas the D-VAT is voluntary.

The VLN can be a stand-alone solution for a single country if there is a heightened concern about MTIC/MTEC fraud. Nothing more is needed than a request for a VLN on importation to set the system in motion. With the D-VAT and RTvat cross-border cooperation is needed. With the D-VAT it is needed *among trading parties,* with the RTvat it is needed *among tax authorities.*

Under the VLN and RTvat a central computer system is the key component, under D-VAT certification a central certification authority is the critical element. None of these solutions comes without an investment in technology but the size of the VAT losses are sufficient to cover the cost of any of these programs.

[45] PKI is information technology infrastructure that enables users of a basically unsecure public network (such as the Internet) to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. In this case the trusted authority would be the Member State that certifies the transaction tax software in the target entity.

[46] A.A.Aronowitz, DCG Laagland & 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,* ¶ 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/ldeucom/101/10105.htm