VAT Fraud and Technological Solutions

By Richard T. Ainsworth

Richard T. Ainsworth is director of international government affairs at ADP Inc. in Salem, New Hampshire. He is an adjunct professor at Boston University School of Law, where he specializes in VAT, and is the former deputy director of the international tax program at Harvard Law School. E-mail: vatprof@bu.edu; Richard_Ainsworth@adp.com.

Every VAT regime is susceptible to missing trader fraud.\(^1\) The fraud is simple and can be easily prevented with the right technology. It arises when a business makes a purchase without paying VAT,\(^2\) collects VAT on an onward sale, and then disappears without remitting the tax collected.\(^3\)

Missing trader fraud is common with high-value/low-volume goods sold across borders; computer chips and cellphones are classic examples.\(^4\) But the fraud easily migrates when pursued. It

---

\(^1\)This is a broad statement intended to include all multistage consumption taxes, such as the European credit invoice VAT, the Japanese consumption tax, and similar VAT or GST regimes, whether at the national or subnational level, as in Canada or Brazil.

\(^2\)There are circumstances in every VAT system when standard business-to-business transactions are made without VAT being charged. Most notable are transactions between EU member states. The standard result is for the purchasing business to self-assess the VAT due with what is called a reverse charge.


\(^4\)House of Lords, European Union Committee, “Stopping the Carousel: Missing Trader Fraud in the EU (Report With Evidence),” HL Paper 101 (May 25, 2007) 7 (indicating that HMRC believed in 2006 that MTIC fraud occurred mainly with cellphones and computer chips). But see Fabrizio Borselli, “Pragmatic Policies to Tackle VAT Fraud in the European Union,” Int. VAT Monitor (Sept./ Oct. 2008) at 333 (observing that data from the Office of National Statistics reported a significant reduction in MTIC fraud adjustments in the first quarters of 2006, corresponding with a rise in U.K. VAT receipts; however, Borselli observes the data reflect only the cellphone and computer chip markets and that MTIC fraud most likely moved to other markets undetected. Indeed, that was the year it moved to the EU carbon permit market, though it was not detected until 2010).
operates well with goods as varied as xenon light bulbs, automobiles, and earth-moving equipment.

**MTIC and Carousel Fraud**

In the European Union, this form of VAT fraud is commonly known as missing trader intra-community (MTIC) fraud. An intra-community goods transaction (that is, a business-to-business sale between EU member states) is the initial sale in the fraud. The initial sale is zero rated so that no VAT is charged on the purchase. Often the same goods participate in the same fraud multiple times, making multiple trips across community borders. In those cases, the goods appear to be on a rotating carousel, hence the less formal name of carousel fraud.

In one widely reported MTIC fraud case, a 21-year-old fraudster appeared to be selling 10 percent of the world supply of a kind of computer chip, when in fact he had only a single box of chips going round and round in U.K.-Irish cross-border trade.

---

5Violetta Krasnowska-Salustowicz and Wojciech Surmacz, “VAT Spins, and We With It,” Newsweek Polska (Mar. 21, 2010) (indicating that the largest tax fraud in Poland involved xenon light bulbs for automobiles; recorded sales for several months were larger than the annual demand in the entire European Union), available at http://www.newsweek.pl/artykul/wydanie/1171/vat-sie-kreci—a-my-z-nim,55162,1 (in Polish).

6Richard T. Ainsworth, “Tackling VAT Fraud: Car Flipping and Computer Chips on a Carousel,” 46 TNI 267 (Apr. 16, 2007) (discussing the largest GST fraud in Canada, involving the sale of automobiles through tax-exempt members of First Nations); Richard T. Ainsworth, “Car Flipping in the U.K.: The VAT Fraud Marketplace and Certified Solutions,” 47 TNI 1157 (Sept. 24, 2007) (discussing how the same fraud in automobiles was replicated in the U.K., but instead of using the GST exemption given to members of the First Nation, the U.K. fraudsters took advantage of the VAT exemption provided to disabled individuals and applied it in sales of high-end automobiles).


Fraud in Services

VAT fraud has recently moved into services. The fraudsters exploit an oversimplification in the definition of taxable supply found in all VAT regimes. It’s common to define goods as tangible property and then to define services as everything else. However, not all services are the same. Some are readily resold like goods, rather than immediately consumed like services.10 This variant of fraud can occur between Norway and Denmark, or Nigeria and Switzerland, or Austria and France. Each of these countries have EU-style place of supply rules for tradable services. The six countries following New Zealand place of supply rules for services are not as vulnerable to this fraud.11

Because missing trader fraud relies on the resale of a supply purchased without VAT, and because most of the early fraud was detected in goods, it’s common to assume that VAT fraud is confined to goods. In fact, missing trader fraud is flourishing among services that are bought and sold like goods (tradable services). It has remained undetected for years.

Services-based missing trader fraud is common for carbon permits, VOIP, and cellphone minutes, and in cloud computing and other areas. The difficulty in fighting services-based missing trader fraud is that the commodity evaporates on use. It is one thing for an auditor to find a box of computer chips riding a carousel, and quite another for an auditor to find VOIP termination minutes that have been repeatedly sold and resold before being fully used.

While it appears there are two classes of taxable supplies (goods and services), in fact there are three: goods, tradable services, and consumed services. The first two are susceptible to missing trader fraud.

10 For example, the EU VAT is imposed on taxable transactions. Those are the supply of goods (the transfer of the right to dispose of tangible property as owner) or the supply of services (any transaction that doesn’t constitute a supply of goods). Art. 5(1), Sixth EC VAT Directive/ Art. 14(1), Council Directive 2006/112/EC and Art. 6(1), Sixth EC VAT Directive/ Art. 24(1), Council Directive 2006/112/EC.

Size of the Fraud

Missing trader fraud is so widespread in the EU that it has distorted national trade statistics in the U.K.\textsuperscript{12} It has been the largest single kind of fraud uncovered in Canada,\textsuperscript{13} Italy,\textsuperscript{14} and Poland.\textsuperscript{15} The Russian mob has long been suspected of involvement in missing trader fraud.\textsuperscript{16} The Ndrangheta mafia, a crime syndicate from southern Italy, uses missing trader fraud to launder money at a profit through the Italian telecommunications system.\textsuperscript{17} Although it is possible to trace missing trader funds and fraudsters from Berlin to Dubai and on to Lahore, Pakistan, there is no direct proof that missing trader fraud is a terrorist funding source.\textsuperscript{18} Some authorities are suspicious about the ultimate destination of the funds.\textsuperscript{19}


\textsuperscript{15}Supra note 5.

\textsuperscript{16}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,” \textit{The Guardian} (May 9, 2006), \textit{available at} http://www.guardian.co.uk/uk/2006/may/09/ukcrime.asheleyseager.


\textsuperscript{18}Reports on the terrorist link in the press can be found generally, but a recent and older report gives some sense of the level of recognition. Paul Fletcher, “Round and Round — From Rags to Riches,” \textit{Commercial Finance Today} (March 18, 2009), \textit{available at} http://www.commercialfinancetoday.co.uk/2009/03/18/mtic-carousel-fraud/; Alan Travis and Ashley Seager, “Reid Wants Europe to Fight VAT Fraud Linked to Terror Funds,” \textit{The Guardian} (Oct. 26, 2006), \textit{available at} http://www.guardian.co.uk/politics/2006/oct/26/eu.terrorism.

\textsuperscript{19}Press Review: Agreement on the European Union to Combat Against So-Called Carousel Fraud Possibly Linked to Terrorism,’’ SEPBLAC — Timesonline (Oct. 27, 2006) (stating, “The six biggest EU states [Britain, France, Germany, Italy, Spain and Poland] have pledged to join forces in the fight against the growing problem of carousel fraud, a multibillion pound tax scam the government believes is linked to terrorism”), \textit{available} (Footnote continued on next page.)
Accurate estimates of the extent of missing trader fraud are unavailable — not for single member states or the EU as a whole. There are no reliable estimates of global losses or country losses in non-EU jurisdictions. In 2006 the U.K. government estimated it had experienced MTIC fraud losses of between £2.98 billion and £4.47 billion. The German government had similar estimates.

During the same 2006 period, Europol’s best estimate for MTIC fraud across the EU as a whole was €23 billion. If we assume that base-line estimate was accurate in 2006, then it is still accurate in 2010. The reason is simple. As explained by Michael Cheetham in his 2006 report to the U.K. House of Lords, one of the most popular solutions to missing trader fraud is a product-specific reverse charge. However, the reverse charge has been adopted by few VAT jurisdictions and is transformative, not curative. The country adopting the standard reverse charge
becomes a base camp for VAT-free supplies that can be sent into
the other jurisdictions.\footnote{Richard T. Ainsworth, “CO\textsubscript{2} MTIC Fraud — Technologically Exploiting the EU VAT (Again),” \textit{Tax Notes Int’l}, Jan. 25, 2009, p. 357 and Figure 3 (Jan. 25, 2009).} Overall the fraud is not reduced, but
maintains the same volume or probably increases in scope.\footnote{The reason fraud may increase is that distribution lines are shortened. Instead of being transported back and forth to Dubai, a two- or three-day journey, the goods can be circulated within the EU with a transit time of a day or less. The carousel simply moves faster.}

Europol’s 2009 estimate of an additional €5 billion in carbon
MTIC fraud in the EU alone should be added to earlier estimates.
Thus, MTIC fraud in the EU has probably risen to at least €28

Reckon LLP studied the so-called VAT gap for the European
Commission in 2009 (also based on 2006 data). The study
indicated that the two most significant research efforts to mea-
sure MTIC fraud were that of HM Revenue & Customs, men-
tioned above, and a study by the Belgian Finance Ministry.\footnote{Reckon LLP, “Study to Quantify and Analyze the VAT Gap in the EU 25 Member
States,” Sept. 21, 2009 (analysis based on 2006 data for all EU member states except
Cyprus), \textit{available at} http://www.reckon.co.uk/item/cb5873cb.} The
Belgian estimates, which also don’t include carbon MTIC fraud, are lower than the Europol estimate for the entire EU (€19.9 billion compared with €23 billion). However, the Belgian esti-
mate for MTIC fraud in the U.K. was considerably higher than
the U.K.’s own estimate (€8.85 billion as compared with the U.K.
estimate of £2.98 billion to £4.47 billion). Reckon can’t explain the
differences.\footnote{\textit{Id.}, at paragraph 383.}

The only reliable conclusion that can be drawn about the size
of the MTIC fraud problem in the EU is that current estimates are
highly speculative and miss entire classes of fraudulent transac-
tions. EU losses are enormous. Because VOIP and other tradable-
services types of missing trader fraud are not confined to the EU,
there is much more to measure. It will take considerable inter-
national cooperation to combat the problem.
The issues raised here affect OECD discussions on harmonizing VAT rules in services and intangibles just as much as they affect EU efforts to combat services and intangibles MTIC fraud in Europe. These issues should be a key policy concern in the United States if there is a sustained effort to design and implement a VAT.

Technological Solutions

MTIC fraud is technology intensive, so it stands to reason that technology-based responses will offer the best solutions.

A transaction in tradable services can be completed in minutes, and the theft of the VAT can occur in the next few minutes. The VAT filing on which the trade is reported might not be due for several months in the future. If the intent is to commit fraud, the funds will pass at lightning speed through a series of domestic and foreign banks. China, Dubai, Hong Kong, India, Pakistan, and Russia are common transit points.

When a cash withdrawal is made on the other side of the world, the stolen VAT becomes impossible to recover, and the supply that supported the fraud has evaporated. The only thing

---


30Aline 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 the author; the average time for a MTIC transaction to be closed out on the BlueNext exchange in Paris is 15 minutes).

31Financial Action Task Force, “Laundering the Proceeds of VAT Carousel Fraud” (Feb. 23, 2007) (see, for example, the £36 million U.K. carousel fraud operation that was based in southern Spain and used Swiss bank accounts, with funds eventually (Footnote continued on next page.)
that slows down missing trader fraud is the nature of the supply — goods must be delivered, and services and intangibles must be made available.

The three leading technology-based solutions will be considered here: the Real Time VAT (RTvat), the VAT Locator Number (VLN) system, and the Digital VAT (D-VAT). There are important differences among them, but generally, the RTvat focuses on securing the tax, the VLN focuses on securely tracing the supply, and the D-VAT certifies that the correct tax is charged, collected, and remitted. RTvat is mandatory for all transactions. In the EU it would have to be adopted throughout the entire bloc. The VLN is also mandatory, but it can be adopted by a single jurisdiction. The D-VAT is voluntary, but it would have to be made mandatory in market segments where fraud is suspected (cellphones, computer chips, VOIP, or carbon permits, for example).

**RTvat**

The RTvat essentially moves the point of taxation from the invoice date to the settlement date. It is also a cash-basis system that mandates debit cards and wire transfers of tax amounts in real time directly to the tax authorities when payments are made. (This proposal considers MTIC in goods, not tradable services.) The key to the RTvat is the network of 27 identical servers — one for each EU member state — that are linked together as transfer centers for communications and funds.
Each EU member state would have to establish a national server system that is separately owned and operated by a national public/private partnership. The private-sector participants would fund the investment and operating costs, and the tax administration would share in any surplus from the revenue stream generated through transaction fees. All VAT payments would have to be made through this system.

The RTvat would change the EU VAT from a withholding system to a direct payment system. Sellers (other than those selling to final consumers) will never hold or otherwise retain the purchaser’s VAT payments. Rather than require sellers to collect and remit VAT, the RTvat would use electronic payments to automatically remove the VAT component from a buyer’s payment and remit that amount to the tax authority in real time. If business X purchased goods from business Y for €100 in a jurisdiction where the VAT rate is 20 percent, X would pay €120. But instead of requiring the seller to collect, hold, and remit €20 in VAT, the RTvat would use the automated payment system to send it directly to the tax authority. The seller will receive €100 (plus a notification that €20 was sent to the tax authority).

Although the RTvat system has never been implemented, automated VAT withholding systems have been in place in Latin American countries for several years. A similar (pre-digital) system was proposed for the EU called the PVAT.

In the Dominican Republic, 30 percent of the tax reported on all VAT invoices paid with a credit card is withheld by the credit card company and remitted to the tax authority. If VAT is not listed on the invoice, the withholding is 100 percent of the tax.

---

38Williams, “RTvat,” supra, note 33 at 7.
39Business-to-consumer transactions would be handled in the traditional manner, with VAT held by the seller and remitted to the tax authority in batches — not transactionally in real time.
40Williams, “RTvat,” supra, note 33 at 7.
41Argentina, Chile, Colombia, Ecuador, Mexico, and Venezuela have systems like this.
42See also the PVAT proposal that requires vendors to collect VAT on all sales, domestic and interstate, with the exception of interstate sales in which the buyer prepays the VAT to the state of destination and provides proof of payment to the vendor. Proof would be a tax deposit receipt. Satya Poddar and Eric Hutton, “Zero-Rating of Interstate Sales Under a Subnational VAT: A New Approach,” in National Tax Association Proceedings: Ninety-Fourth Annual Conference (2001) 200-07.
The seller is notified that a VAT payment has been made on his or her behalf. Puerto Rico’s sales tax may change to the same withholding regime so that the full amount of the tax would be due on all invoices paid with credit or debit cards.

The RTvat proposal anticipates a staged rollout, with the first stage confined to domestic transactions in a member state and a second stage when intra-community transactions are handled. Only during the second stage would MTIC fraud be eliminated. This stage would require a single VAT registration across the EU.

MTIC is eliminated with the RTvat because a business buyer would always pay domestic VAT on purchases, even those made across intra-community borders. In the example above, €100 will be remitted to the cross-border seller, and €20 will be sent directly to the buyer’s jurisdiction. There will be no reverse charge. Cross-border sales will be taxed at the applicable rate in the buyer’s jurisdiction, not zero rated by the seller in the expectation that the buyer will perform a reverse charge.

The RTvat would affect businesses that take advantage of cash flow opportunities under the current system. It would require the immediate payment of VAT on value added at each stage of production, and some businesses would have to finance the VAT. That is particularly the case in a down economy where inventory is purchased but not easily resold. The RTvat will also not eliminate B2C frauds — for example, the use of automated sales suppression technology at the point of sale to skim cash sales (for example, so-called zappers and phantomware applications). Of the three technology solutions considered here, only the D-VAT could provide that kind of comprehensive fraud prevention.

---

43 Decree (DR) 140-98; Tax Code (DR) 11-92; General Regulations (DR) 02-05 and 08-05.
VLN

The VAT Locator Number system is the simplest of the three solutions to adopt. It’s also the least disruptive to the current VAT system. Statutory changes would be minimal. Its creator, Michael Cheetham, proposed it at the May 25, 2007, House of Lords hearings.46 The VLN solution is targeted — it prevents only MTIC fraud.

The most significant policy change under the VLN proposal would be the denial of a buyer’s input credit if a seller pays VAT on an invoice with an invalid VLN (or an invoice with no VLN at all). The most significant procedural change is that businesses would need to secure a VLN when selling supplies, or validate an opposing trader’s VLN when purchasing supplies. Accounting software platforms would usually make automated requests for VLNs from the government’s central computer system and make automatic validation requests in the same manner. Each link in the commercial chain would be given a number, and the numerical sequence would follow the goods or services from initial manufacture through to final consumption. A backup system whereby VLNs could be secured through a website or a call center would be available.47

The VLN system requires the seller on each transaction to secure and print on the invoice the encrypted VLN. The number would be unique to the transaction (based on the essential data elements of the invoice and prior related VLNs from transactions up the commercial chain). The VLN number would be attached to the invoice, either numerically or as a bar code that could be scanned and read with an optical reader.48 The advantage of a bar

46Supra, note 34.
47Michael Cheetham, personal e-mail communication (Apr. 25, 2010) (on file with author).
48A similar bar code will be added to each cash register receipt issued by Quebec restaurants under their enforcement effort directed against zappers. The sales recording module 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 handheld optical scanner. That will allow inspections whereby during a 30-minute visit an auditor 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 (Footnote continued on next page.)
code and optical reader capabilities is that a trader could 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 reliable. In Brazil invoices receive a digital bar
code at the interstate border from a federal computer feed. The
bar code is used to validate the invoice and the physical transit of
the goods.49

Two examples of the VLN may be helpful. The first involves a
standard cross-border sale within the EU. The second shows
what happens if a trader sells without a VLN. The response of the
next trader in line to the lack of a VLN is to pay all the VAT to the
tax authority to secure a VLN that will allow him to continue
reselling the purchased supplies. No VAT is paid to the business
that sells without a VLN. MTIC fraud is eliminated, and the
commercial chain continues uninterrupted. It is expected that the
merchant that sold without a VLN would be penalized (and that
business may find it more difficult to secure a VLN in the future
because a risk assessment would suggest that it needs more
careful oversight).

Example #1: VLN Import

A business in France (B1) sells goods or a service to a business
in the U.K. (B2). B1 zero rates the sale, and B2 requests a VLN (for
the reverse charge) from HMRC (VLN-1). The VLN request will
include the essential elements of the invoice received from B1.
HMRC performs a risk assessment, and if B2 is deemed a
low-risk importer (the risk we are concerned with is whether B2
is likely to go missing), a VLN number will be issued.

Bernard, “Solutions for the Underreporting of Income in the Restaurant Sector,”
Federation of Tax Administrators Annual Conference, Denver (June 2, 2009), PowerPoint
slides at 15-17 (on file with author).

49Several Brazilian states and the federal government signed an agreement on Sept.
30, 2005, to create (1) the e-invoice and (2) the auxiliary document of the e-invoice. Ajuste
20, 2005, through the ATO Cotepe/ICMS N.72 de 20 de Dezembro de 2005 http://
www.sef.rj.gov.br/legislacao/tributaria/convenios_ajustes_protoclos/confaz/parecer
es_ecf/2005/ato072_05.shtml, the structure of the e-invoice was established and testing
was initiated with 19 companies and those companies and six states. The program has
been deemed a success and has been extended.
VLN-1 is an encrypted identifier that will be the basis of subsequent VLN-2s, which will be necessary when B2 sells the goods or service to another U.K. business (B3). The B2/B3 transaction is accompanied by VLN-2, which will be requested by B2. VLN-2 includes within its encryption base not only data related to the B2/B3 transaction, but data from VLN-1. That allows for the construction of a digital trail. B3 will not be allowed a deduction for VAT paid if there is no VNL on the invoice B3 receives, or if the VLN it receives on the invoice is invalid.

Example #2: Sale Without Valid VLN

As before, a business in France (B1) sells goods or a service to a business in the U.K. (B2). B1 zero rates the sale, and B2 applies for a VLN for the reverse charge. B2 receives VLN-1 from HMRC after a risk assessment determines that B2 is a low risk to go missing.

B2 resells to another U.K. business (B4) without securing a resale VLN. In this situation, B4 would be unlikely to pay VAT to B2, because B4 would be denied a VAT deduction for the amount paid. If B4 wants to complete the trade, it will pay the VAT directly to the U.K. Treasury, effectively performing a reverse charge. B4 would now receive (from HMRC’s computer system) a VLN number that will allow it to deduct the VAT on any future resale.

When a resale occurs (B4/B5), there is a request for a VLN for the transaction. (It may be that quantities are different for the B2/B4 transaction; changes could have been made in the product.) With the new VLN, which relates back to the VLN that B4 and B2 received from HMRC, it is possible to make a sale to B5, impose domestic VAT, and remit it normally.

D-VAT

MTIC fraud can be eliminated by the use of certified tax software and a conditional change in the standard place of supply rules. Certified tax software is being used by 23 U.S. states to manage retail sales tax under the Streamlined Sales and Use Tax Agreement.
**Figure 1.**

VLN-1 & 2 – encrypted numeric & scanned bar code on invoice identifying vendors, goods, & trail. One number merges all data.

Automated request for a "reverse charge" VLN followed by a request for a resale VLN (essential elements of invoice)

1. Goods/service code
2. Quantity
3. Price paid
4. Vendor ID
5. Vendee ID

Confirming the VLN – OK to pay VAT?
Automated request for an import/"reverse charge" VLN (essential elements of invoice)
1. Goods/service code
2. Quantity
3. Price paid
4. Vendor ID
5. Vendee ID

Figure 2.
Tax Agreement.\textsuperscript{50} The same software mechanisms could be applied to VAT to fight missing trader fraud.

Like the VLN proposal, D-VAT changes the place of supply — and thereby the party that was required to remit the tax — based on whether the businesses involved in the transaction used certified tax software. Under VLN, the determinant is whether a valid VLN code appears on the invoice.

A testing regime for the certification of enterprise-level trans-action tax software is required under a D-VAT.\textsuperscript{51} The software must be comprehensive and able to:

\begin{itemize}
  \item determine the correct tax for each transaction;
  \item post that amount on the appropriate invoice;
  \item link each VAT input or output amount to the correct VAT return; and
  \item complete the VAT return accurately.
\end{itemize}

Certified tax software also must verify whether the companion system used by the other trader is also properly certified.

Business use of certified tax software would be voluntary. In some instances a jurisdiction might make use mandatory — for instance, when an enterprise is heavily engaged in transactions


deemed prone to missing trader fraud (emissions permits, cellphones, computer chips, etc.). In judicial proceedings, the government could seek the use of certified software by some traders because of proven instances of fraud in the past.52

If a jurisdiction were to adopt a D-VAT, four permutations of the software must be considered. Assume a taxable transaction occurred between taxpayers A and B, which are in different jurisdictions. It could be the sale of goods or tradable services among EU member states, or a sale of tradable services between any two VAT jurisdictions.

Under standard VAT rules, the transaction would be zero rated on leaving A’s jurisdiction and subject to a reverse charge entering B’s jurisdiction. If B is using a certified system, there should be no problem with the transaction. A certified system will always perform a required reverse charge regardless of the certification of the other party’s system. B’s VAT return will be properly prepared along with all related reports, and the funds will be properly remitted to the government. A problem might arise only when A is not using a certified system.

The following illustrations summarize these applications.

Fact Pattern 1: A Certified; B Certified

If A and B both use certified tax software systems, the zero rating and reverse charge will be properly made and reported and the VAT payment remitted to B’s government. That would be the outcome even if the transactions involved suspect classes of supplies (cellphones, computer chips, carbon permits, VOIP, etc.).

52 This was the approach Judge Lise Gaboury of the Court of Quebec took in the fraud case against the restaurant chain Casa Grecque. 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 March 23, 2006, budget speech, the minister of revenue announced the adoption of an automated system [module d’enregistrement des vents] that would be voluntary until 2011. Judge Gaboury required all the Casa Grecque restaurants to adopt it 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.
Fact Pattern 2: A Uncertified; B Certified

If A is not using a certified tax software system and B is, then B will reverse charge. The only question is whether A’s jurisdiction will allow zero rating. B’s certified system will perform a reverse charge. If A was engaged in the supply of a suspect industry, zero rating could be denied. (If not, zero rating might be allowed under traditional VAT rules.) The issue likely is whether A’s jurisdiction is willing to accept B’s certification as proof that A had fulfilled a due diligence obligation to verify that B was not participating in missing trader fraud. If so, A should be allowed to zero rate the sale.

Fact Pattern 3: A Certified; B Uncertified

If A is using a certified system and B isn’t, A’s system would recognize that and wouldn’t zero rate the transaction if it involved a suspect class of supplies. Instead it would impose the domestic tax. B would then be in a difficult situation. B’s purchases would be burdened with the VAT of another jurisdiction, and it would remain obligated to comply with the reverse charge in its own jurisdiction. Double taxation would result, unless B could obtain a refund in A’s jurisdiction (which is procedurally complex). B would most likely seek a domestic supplier, which would charge domestic VAT, or change its status by installing a certified tax software system. The latter is the desired result for the treatment of suspect classes of supplies.

Fact Pattern 4: A Uncertified; B Uncertified

If neither A nor B is using a certified tax software system, the question is whether the transaction is deemed to involve a suspect class of supplies. If A’s jurisdiction considers the trade in cellphones a suspect activity, it should make all cellphone transactions taxable at regular rates (domestic and cross-border). A will not be allowed to deduct VAT paid on cellphone purchases, and it will have to collect VAT on all cellphone sales. Also, B’s jurisdiction will require VAT to be collected under a reverse charge.

In a D-VAT regime that is extended throughout a federal system, it is expected that notifications of certified status between automated systems would be automatic and handled through a secure online connection. Dual notifications would be expected
under some conditions. All of that could occur almost instantly. There are various ways to do this, but the most proven and secure would be through the use of public key infrastructure (PKI).\(^5\) A’s system would access the public key associated with B and use it to confirm that B’s system was certified. A would then draft an invoice without VAT and forward it to B. That way A would know that B’s system would perform the reverse charge.

In one sense, this process is simply automated due diligence. In another, it is certified due diligence. For the sake of caution, it is expected that B’s certified system will perform a reverse PKI inquiry when it is notified that A’s system is checking for certification. B’s system would want to determine in advance that the invoice it’s receiving from A (without VAT) is correctly issued.

**Conclusion**

The recent appearance of MTIC fraud among tradable carbon permits and VOIP is a warning for the global VAT system. The size and scope of the fraud make it clear that it is a huge problem that is spreading. The speed at which it spreads is a reflection of the technology that makes it work. In tradable services, it has no boundaries.

Three technology solutions are presented here and summarized as follows:

- The RTvat is applied to all transactions in a VAT system. It changes the underpinnings of the VAT, moving it from an invoice system to a settlement system. The withholding-and-remit element of a VAT system has been effectively removed.
- VLN also applies to all transactions in a VAT system but leaves the basic structure of the VAT untouched. It simply adds an encrypted tracer code to every invoice.

\(^5\)PKI is an information technology infrastructure that enables users of a basically non-secure public network (such as the Internet) to securely and privately exchange data through the use of a public and 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.
The D-VAT accomplishes much of what the VLN does, but uses certified tax software. The D-VAT can be applied selectively to suspect classes of supplies. It’s also voluntary (with several incentives to get businesses to sign up). It is the only solution that can be extended to cover B2C transactions.

If the United States is serious about adopting a VAT, it must consider VAT-related fraud. Congress would be wise to preempt the problem before the tax is ever enacted. Technology must be placed at the service of the tax collector, not the fraudster.