#### **Boston University School of Law**

### Scholarly Commons at Boston University School of Law

**Faculty Scholarship** 

11-2020

### Afghanistan's New VAT, Part 1: Invoice Matching or a Unitary Digital Invoice

Richard Thompson Ainsworth

Musaad Alwohaibi

**Andrew Leahey** 

Yujin Li

Haseena Rahman

Follow this and additional works at: https://scholarship.law.bu.edu/faculty\_scholarship

Part of the Banking and Finance Law Commons, Business Organizations Law Commons, Law and Economics Commons, and the Tax Law Commons



Volume 100, Number 9 ■ November 30, 2020

by Richard T. Ainsworth, Musaad Alwohaibi, Andrew J. Leahey, Yijin Li, and Haseena Rahman

Reprinted from Tax Notes International, November 30, 2020, p. 1211

## Afghanistan's New VAT, Part 1: Invoice Matching Or a Unitary Digital Invoice

by Richard T. Ainsworth, Musaad Alwohaibi, Andrew J. Leahey, Yijin Li, and Haseena Rahman







Musaad Alwohaibi



Andrew J. Leahev



Yijin Li



Haseena Rahman

Richard T. Ainsworth is an adjunct professor at the Boston University graduate tax program and the New York University graduate tax program. Musaad Alwohaibi is a professor of international taxation law at the College of Law and Political Science, King Saud University. Andrew J. Leahey is a tax and technology attorney in New Jersey. Yijin Li is an attorney at DeHeng Law Offices in Beijing. Haseena Rahman is the director of the Special Anti-Corruption Secretariat at the President's Office in Kabul.

In this article, the first in a three-part series, the authors discuss the choices Afghanistan faces as it implements its first VAT and, in particular, how it can prepare to fight VAT fraud. They review the problem of VAT invoice fraud, examine the traditional use of invoice matching to combat the problem, and begin to consider how technology can help, including the potential use of business process reengineering.

In the summer of 1990, two groundbreaking articles on business process reengineering (BPR) captured the attention of academics and business professionals alike: The publication by lead author Thomas H. Davenport, a professor of information technology at Babson College, and his coauthor James E. Short of the Massachusetts Institute of Technology appeared in the MIT Sloan Management Review;<sup>1</sup> and Michael Hammer, a

professor of computer science at MIT, published his article in the *Harvard Business Review*.<sup>2</sup> The publications were coordinated, and the lead authors had decades of both academic and technology consulting experience. BPR is a management strategy that analyzes IT-intensive workflow designs and business processes within an organization. Initially, BPR was used to help private companies radically restructure around IT.

<sup>&</sup>lt;sup>1</sup>Davenport and Short, "The New Industrial Engineering: Information Technology and Business Process Redesign," 31(4) *Sloan Mgmt. Rev.* 11 (Summer 1990).

<sup>&</sup>lt;sup>2</sup>Hammer, "Re-Engineering Work: Don't Automate, Obliterate," *Harv. Bus. Rev.* 104 (July-August 1990).

Since then, BPR has changed and expanded the way we think about IT. By 1997 the U.S. government was using BPR to help guide the restructuring of large public institutions.<sup>3</sup>

Hammer's wording tends to be harsh, but his commitment to the field runs deep. He advocates obliterating all forms of work that do not add organizational value. Specifically, Hammer opposes the use of technology simply to automate older work models. Far too often, he observes, IT is used to automate existing processes without management taking the time to consider what could be accomplished if IT was treated as a core business attribute.

Davenport doubles down on Hammer's insights. He emphasizes a holistic focus on business objectives and strives to identify how IT processes relate to those goals. He supports using IT for full-scale re-creation rather than for the iterative optimization of subprocesses.

Afghanistan plans to implement a 10 percent VAT beginning December 21. To do so, the country will have to make significant workflow design and business process decisions. There will be problems, of course, but there are also great opportunities. The question for Afghanistan is not whether it will apply information technology in VAT administration, but rather how it will design workflows and business processes given today's technology. In an article published earlier this year, Bilal Hassan (an official with Pakistan's Federal Board of Revenue) underscored the importance of IT in the Afghan VAT, stating:

Strengthening the administrative capacity of the tax authorities and using information technology (IT) will be crucial for ensuring VAT compliance.<sup>4</sup>

This article, the first in a three-part series, undertakes a limited, comparative study of VAT invoices. It applies BPR principles to the invoice

#### The Reality of VAT Fraud: An Overview

The Afghan VAT is a standard credit-invoice VAT of European vintage. Like all credit-invoice VATs, it operates on an invoice-matching principle: The input VAT — paid by the buyer and referenced on a purchase invoice — should be directly traceable to an identical amount of output VAT collected by the seller and counterreferenced on the sales invoice. If everything matches on all invoices, for all transactions in the jurisdiction, there is no fraud — or, more accurately, there should be no fraud. As part 2 of this series will note, specifically in the context of the Shanghai case, sometimes fraudsters use invoice matching to disguise fraud.

Given the number of transactions and the amount of VAT involved, we can be sure that there will be fraud attempts and successes in Afghanistan. In 2017 the VAT gap in Europe totaled €137.5 billion, and it is safe to say that the vast majority was a result of fraud. The methods used to carry out VAT frauds are no secret. Just like it does in the EU, fraud will occur on both sides of Afghan transactions with fraudsters using fake invoices on the purchase side and missing traders on the sales side. The goal is to minimize fraud — expecting to eliminate it may be unrealistic, especially for a new VAT jurisdiction — and technology can help.

On the purchasing side, fraudsters use fake invoices to secure refunds of VAT that was never paid on supplies that were never bought. In contrast, supply-side fraudsters make real sales

function of a credit-invoice VAT, and it offers an assessment that looks at where the leading edge of this element of VAT practice is today. Our hope is that this analysis proves useful to officials in Afghanistan or another jurisdiction that is adopting a new VAT.

<sup>&</sup>lt;sup>3</sup> See, e.g., U.S. General Accounting Office, Business Process Reengineering Assessment Guide (May 1997).

<sup>&</sup>lt;sup>4</sup>Hassan, "The Challenge of VAT Implementation in Afghanistan," 30(2) *Int'l VAT Monitor* 80 (Mar. 2019). Notably, however, Hassan views invoice workflows and processes in terms of matching rather than a unitary digital invoice:

The tax authorities need to implement the VAT system strategically and ensure effective supervision through audit and fraud control measures with the aid of obtaining information from the cross-matching of data. [Emphasis added.]

<sup>&</sup>lt;sup>3</sup>See Graham Harrison and Russell Krelove, "VAT Refunds: A Review of Country Experience," IMF Working Paper WP/05/218 (Nov. 2005) (noting "the theoretical possibility that a tax administration should be able to cross-check all purchases and sales invoices to validate VAT credit claims (as well as identify undisclosed sales)"). See also Alan Schenk, Victor Thuronyi, and Wei Cui, Value Added Tax: A Comparative Approach (2015) (on the centrality of the VAT invoice to a European-style VAT).

<sup>&</sup>lt;sup>6</sup>Center for Social and Economic Research, "Study and Reports on the VAT Gap in the EU-28 Member States: 2019 Final Report," TAXUD/ 2015/CC/131 (Sept. 4, 2019).

and collect real VAT, but when the time comes for a return to be filed, either selective transactions are omitted or the supplier itself disappears, taking the VAT along with it. In either case, government auditors spend considerable time and effort proving fraud — after the fact — by examining paired invoices. This is the invoicematching principle in practice at the auditor level. If Y purchased what X sold, then the invoice records on both sides should match. Fake invoices, missing transactions, and missing traders point to fraud.

Invoice matching is often the most essential tool for auditors in a fraud investigation. When compliance was not in real time — when it involved paper invoices and paper returns filed one to three months after the underlying transactions occurred — a suspected fraud case meant government auditors had to sift through piles of paper invoices to check for mismatches. The need to automate the invoice-matching function was obvious.

#### **Examples of Invoice Fraud**

Throughout this series of articles, we will use three examples to illustrate differences among VAT systems. The first two examples involve reasonably common fraud patterns: Abdul Majeed's fake invoice fraud, which totaled £119,624, and Sandeep and Pardeep Dosanjh's three sequential missing trader frauds (respectively totaling €31,244,175; €9,795,086; and £11.7 million). The third example is from Shanghai (CNY 250 million, roughly \$35 million); it involves a newer kind of fraud that hasn't been paid much attention yet, but it is probably more common in practice than observers realize. The Shanghai fraud example will be considered in part 2 of this series.

#### Example 1: Abdul Majeed

Majeed served as the company secretary for two fashion firms located in the United Kingdom. His fraud was decidedly low-tech: It involved the production of numerous fake invoices, and it escaped the detection of HM Revenue & Customs for nearly eight years. Majeed's fraud was successful, in part, because of natural mistakes stemming from the similarity of the names of the companies he used for four of those years: Majtex

Ltd. (incorporated April 23, 2007) and Majtex International Ltd. (incorporated May 7, 2009) were both VAT registered, the Companies House had assigned each entity a number (the registration system for limited companies in the United Kingdom), and they had different physical addresses. But Majeed's success was also the result of strategic manipulation. He was remarkably good at selectively doubling input VAT deductions.

An HMRC release describes the fraud,<sup>7</sup> and additional details from other public documents make HMRC's rough sketch clearer. HMRC indicates that Majeed used legitimate suppliers' invoices as templates to create fake sales and purchase documents. The fraud, which involved three basic fact patterns, occurred from April 2006 through April 2014. This timespan can be broken down into the following four periods:

- April 2006-April 23, 2007: Before the incorporation of either of his businesses, Majeed appears to have been engaged in the fashion textile business as an individual trader. HMRC indicates that Majeed first employed fake purchase invoices in this context to obtain excess input credits.
- April 23, 2007-May 7, 2009: Majeed continued to produce fake invoices after incorporating Majtex Ltd.
- May 7, 2009-October 22, 2013: During this period, Majeed operated brother and sister companies namely, Majtex Ltd. and Majtex International Ltd. The pattern of fake invoices became more complicated with purchase and sales invoices passing between his own companies and disguising other fake transactions, some of which were international.
- October 22, 2013-April 2014: In this final period, HMRC had discovered the fraud and asked Majeed to come clean and explain invoice irregularities. The offer, a contractual disclosure facility, would have prevented a criminal investigation if Majeed had responded to it in good faith within 60 days. Instead, he ignored HMRC's request

<sup>&</sup>lt;sup>7</sup>HMRC, "Clothing Wholesaler Sentenced for VAT Fraud" (Oct. 9, 2018).

and dissolved Majtex Ltd. without admitting fraud. HMRC opened a full criminal investigation, which resulted in Majeed's pleading guilty in Manchester Crown Court, a two-year suspended sentence, community service, and various financial compensation orders reaching £120,000.

#### Majeed's First Fact Pattern

Majeed purchases textiles from U.K. suppliers in his own capacity and later through Majtex Ltd. He pays U.K. VAT and receives a valid VAT invoice. This valid invoice is cloned, and Majeed creates a second invoice for essentially the same purchase. On his VAT return, Majeed records deductions for all the VAT that all the invoices — genuine and cloned — suggest was paid, thus deducting more input VAT than he actually paid.

Majeed's cloning technique did not involve exact replicas; he included minor differences in the cloned invoices to disguise the duplication.

#### Majeed's Second Fact Pattern

This pattern is similar to the first. A legitimate purchase invoice is cloned to produce an additional, fake purchase invoice. The fake invoice references a fake textile purchase by Majtex Ltd., which that company then resells to Majtex International Ltd. Finally, a third fake invoice is produced indicating that the fake textile purchase is exported, thus resulting in a refund for VAT that was never paid. Majeed also ran the same pattern in reverse, cloning Majtex International Ltd.'s purchase before making a fake sale to Majtex Ltd.

Two frauds occur in the original version of this second pattern. First, Majtex Ltd. takes a double input VAT deduction for a single purchase. Second, Majtex International Ltd. requests a VAT refund for a fake zero-rated export. Importantly, if Majtex International Ltd. was audited, it could provide its purchase invoice, and the group could also supply Majtex Ltd.'s matching sale and earlier purchase invoices.

This second Majeed fact pattern shows fraudsters' tendency to construct fake commercial patterns of matched invoices to obscure the real fraud. The Shanghai fraud, discussed in part 2, involves the same thing on a much larger scale — \$35 million.

#### Majeed's Third Fact Pattern

The third pattern was Majeed's mistake. HMRC discovered his invoice frauds when he began cloning import invoices.

Majtex International Ltd. imported clothing from outside the EU. It paid import VAT to customs at the port of entry and received a customs form (C79) as proof of payment. Majeed would then clone the (Majtex International Ltd.) invoice and, relying on the similar names, pretend that Majtex Ltd. had made an import. Both companies claimed input VAT deductions based on a single import and the same VAT payment. Majeed supported both the real invoice to Majtex International Ltd. and the fake import invoice to Majtex Ltd. with the same C79. However, customs uncovered the fraud using its C79 cross-check program.

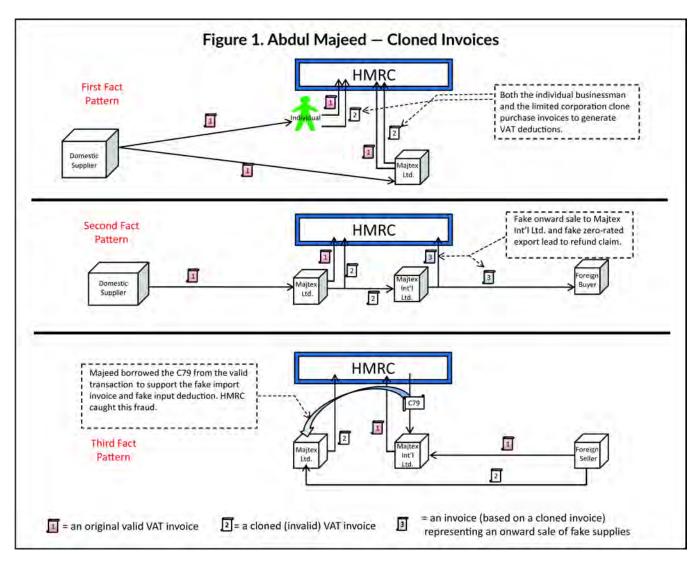
Figure 1 diagrams each of Majeed's fact patterns.

#### **Example 2: The Dosanjhs' Fraud Bot**

This example involves missing trader fraud. It is different in almost all respects from Majeed's fake invoice fraud. The Dosanjh fraud is a fully automated, fast-moving, large-loss fraud, and it involves a tightly knit criminal gang of family members. Fraud chains are designed to last days, normally ending before the time for the filing of the first VAT return. In contrast, Majeed's fraud was a low-tech, one-man, fully manual cloning fraud, and it produced modest loss-to-revenue returns for nearly a decade.

The Dosanjhs created a fraud bot that needed very little human intervention. Fraud bots are most effective with intangible (digital) properties such as CO<sub>2</sub> emissions permits, gas, electric, voice over internet protocol rights, and telephone calling cards. In this case, the bot could be (and, in some instances, was) operated from entirely outside the creators' home country (the United Kingdom).

Missing trader frauds typically involve a chain of companies controlled by a fraudster and his associates. With a fully operational fraud bot this control is remote. The first company imports a supply — CO<sub>2</sub> permits, in the Dosanjh example — and resells it along the chain for a small profit at each stage, with the last company exporting the



supply. Each company pays a small net VAT, with two exceptions:

- The first exception is the initial company in the chain. It is supposed to remit a large VAT payment on import using a reverse charge. However and this is the heart of one of the most common VAT frauds the company does not perform this reverse charge and goes missing before its VAT return is due. The same company also keeps all the VAT it receives on its forward sales (undiminished by a reverse charge).
- The other exception is the exporting company. This entity can apply for a refund because consumption is expected to happen outside the jurisdiction.

The profit, which is typically split using a formula, is the combined total minus expenses and the small net VAT paid along the chain.

In the Dosanjh case, which resulted in multiple appellate decisions:

The proceeds were swiftly moved offshore into "banking platforms," in particular, commercial banks in Hong Kong, Australia, and New Zealand. These operated in a manner described as being "analogous to a solicitor's client account." All the money went into one account but there were internal ledgers used to allocate it between the "sub-accounts" of the traders. This meant that the true nature of the transfers was effectively disguised and difficult to detect.<sup>8</sup>

<sup>&</sup>lt;sup>8</sup>R. v. Dosanjh, [2013] EWCA Crim 2366. See also R. v. Chada, [2016] EWCA Crim 1955.

Court decisions identify Sandeep Dosanjh and his second cousin Pardeep Dosanjh as the "prime organizers and main beneficiaries" of this technologically sophisticated missing trader fraud. Three rapidly executed, sequential permutations of this fraud cost the U.K. Treasury a total of €52,739,261. On August 19, 2009, an attempt was made to arrest all the conspirators, but Pardeep Dosanjh fled the jurisdiction before he could be arrested. As of the drafting of this article, he had not been extradited (papers are outstanding).

The technology that enables this fraud works like digital origami. Fraud chains are put into place and then folded back up and moved away when no longer needed. As the appeals court explained in 2013, "The chains and money laundering arrangements were all set up in advance so that new companies and new banking arrangements could be used as and when required without causing any disruption in the fraud."

When it identified the Dosanjh fraud, HMRC tried to stop it in four different ways. The first three efforts involved blocking foreign money transfers, blocking domestic trading activity, and zero-rating all trade in CO<sub>2</sub> permits. The final remedy was arresting the Dosanjh cousins and all known associates and holding them in jail without bail for a year. The goal of the arrests and detentions may have been to secure the Dosanjhs' technology, but there are indications that the technology had already been transferred to other fraudsters — notably gangs in Germany, some of which had long U.K. associations.

It is apparent that even the final remedy of arresting everyone and confining them to jail cells was not a complete solution. New associates were easily found to continue the fraud. When it sentenced the responsible parties in the third iteration of the chain in 2016, the court noted that "none of these three defendants was involved in that first fraud" — that is, none of the defendants involved in the third chain was involved in chains one or two. The real problem isn't the people it's the technology, the fraud programming, and the system of digital origami that allows operators to move any entity or individual in or out of the system on demand. The fraud continues while the operators change. The real fraudster is the fraud bot, and one of the biggest dangers is the fact that it can be controlled from anywhere in the world.

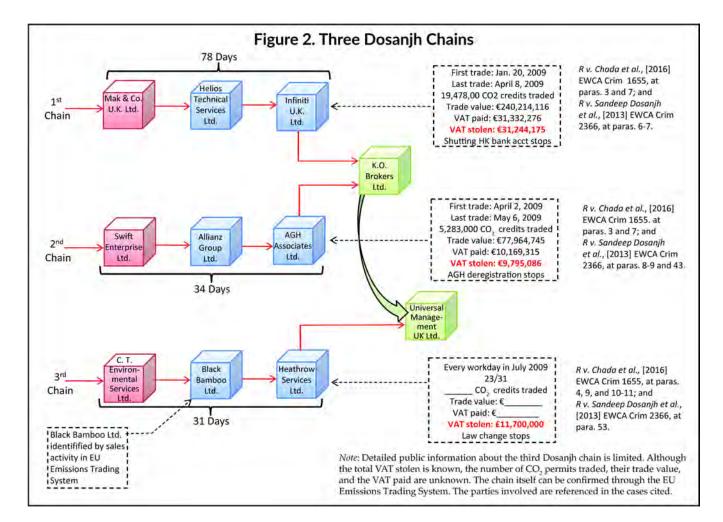
HMRC's first attempt to stop the Dosanjhs' first fraud chain involved asking the Hong Kong banking authorities to disrupt the payment platform. It worked, but only briefly. The fraudsters quickly moved the payment platform to New Zealand and changed each of the companies in the fraud chain. There was no gap in fraud operations. The second fraud chain overlapped with the first for six days, from April 2 to April 8, 2009, and then the new chain continued on.

The first chain operated for 78 days before the second chain took over, using different companies, different directors, and different overseas banking arrangements. It lasted 34 days. When HMRC identified the switch, it decided not to wait for New Zealand's banking authorities to shut down the second chain's payment platform. Instead, HMRC shut down the penultimate company in second chain, the company that supplied CO<sub>2</sub> permits to the Dosanjhs' final company (KO Brokers Ltd.) and was poised to either export or sell permits domestically. This entity, AGH Associates Ltd., is commonly called the final buffer.

After a month-long pause — notably, the same month when the BlueNext exchange in Paris was shut down for rampant CO, fraud and when France exempted  $CO_2$  permits from VAT — a third Dosanjh chain began operating in the United Kingdom. Once again, the Dosanjhs' fraud bot had simply substituted different companies, different directors, and different overseas banking arrangements. The fraud continued. Even the final link in the chain was changed to a new company that was owned by a new fraudster, a third Dosanjh cousin, Gurmail Dosanjh. The third chain lasted for 31 days and, as the 2016 decision reports, "trading on every working day in July 2009, the third chain resulted in a loss to the Revenue of £11.7 million."

HMRC realized that it could not stop the Dosanjhs' fraud bot. The only effective course of action was to change the law and zero-rate CO<sub>2</sub> permits. This change took effect August 1, 2009.

HMRC, "VAT: Zero Rating of Emissions Allowances With Effect From 31 July 2009," Brief 46/90 (July 30, 2009); and David Connett, "Carbon Credit Scam Would Have Cost Britain £2bn," The Independent, June 24, 2012.



With this change, the Dosanjhs' fraud bot finally stopped operating — at least in the United Kingdom. This leads one to ask: Where could it have been installed next? That, however, is beyond the scope of this article.

Figure 2 diagrams the three Dosanjh fraud chains in the United Kingdom.<sup>10</sup>

#### Can Invoice Matching Solve VAT Fraud?

The credit-invoice VAT is designed around invoice matching. Advocates of the system say invoice matching makes the tax self-enforcing.<sup>11</sup>

However, with 2017 data<sup>12</sup> indicating a €137.5 billion (down from €145.5 billion) VAT gap in the EU, many feel that this "self-enforcement" is overstated.<sup>13</sup> Visible oversight is still needed for an efficient and effective VAT. Normally, audits — real and physical or remote and digital — are needed.<sup>14</sup>

Normally, an auditor's first step in a VAT fraud case would be to attempt to match invoices. Invoice matching would detect Majeed's fake invoices; they matched nothing, so the fraud was

<sup>&</sup>lt;sup>10</sup>For diagrams including the major commercial purchasers of CO<sub>2</sub> permits from the Dosanjh chains and the various payment platforms, see Richard T. Ainsworth, "VAT Fraud Mutation, Part 1: 'Push' Missing Trader Fraud and Dosanjh," *Tax Notes Int'l*, Feb. 8, 2016, p. 535.

<sup>&</sup>lt;sup>11</sup>See, e.g., European Union, "Green Paper on the Future of VAT — Towards a Simpler, More Robust and Efficient VAT System," COM(2010) 695 final (2010). The classic academic study advancing this principle is Cedric Sandford and Michael Godwin, "VAT Administration and Compliance in Britain," in Value Added Taxation in Developing Countries (1990).

<sup>&</sup>lt;sup>12</sup>Center for Social and Economic Research, *supra* note 6.

<sup>&</sup>lt;sup>13</sup>Ben Terra, "The European Court of Justice and the Principle of Prohibiting Abusive Practices in VAT," in *GST in Retrospect and Prospect* (2007). *See also* Joep Swinkels, "Carousel Fraud in the European Union," 19(2) *Int'l VAT Monitor* 103 (2008).

<sup>&</sup>lt;sup>14</sup>See Arindam Das-Gupta and Ira N. Gang, "Value Added Tax Evasion, Auditing and Transactions Matching," Rutgers University WP 96-07 (1996).

detected. Invoice matching would also identify Dosanjh's missing traders — the invoices that the buffer entities received when they made purchases from missing traders would have no match. Again, the fraud was detected.

Applied case by case, invoice matching works well. But it is not a complete answer for all situations; it takes time, and invoice matching an entire VAT system is a daunting task. The process picks up clerical mistakes, minor errors, and numerical transpositions in manual entry documents. Jurisdictions that have tried to manually match all invoices — the IMF puts Algeria, Azerbaijan, Bulgaria, China, Indonesia, Korea, and Taiwan in this group — have failed.

However, in the 1990s, these failures were not seen as a defeat. Instead, the efforts were seen as indications that victory was at hand. Supporters believed that if programming was perfected and computers became faster, then true selfenforcement could be — and would be realized. As a World Bank study by Arindam Das-Gupta and Ira N. Gang concluded:

What is surprising, however, is that even if the STA (State Tax Authority) is inefficient in carrying out audits, intensive crossmatching under the assumption of a known technology can lead to fullcompliance with the VAT as a consequence of self-enforcement. This situation may become possible when the cost of cross-matching is low due to the deployment of high-speed computers.<sup>15</sup>

Given what we know now about BPR, this is an extraordinary statement. Can the VAT have full compliance through self-enforcement, if intensive cross-matching (a standard audit practice) is applied with a known program? Is access to highspeed computers the only condition? Is the right answer getting faster computers to replicate auditors? This is not BPR.

Thus, we arrive at the 1990s intersection of VAT administration and BPR. In 1996 Das-Gupta

and Gang reached a conclusion that is the exact opposite of what Hammer and Davenport hypothesized in 1990. There is a fork in the road ahead. There is a considerable difference between the idea that "all we need is higher-speed computers" and a philosophy that says "what we need is re-engineering of business processes around the present capabilities of IT."

What is even more striking for purposes of this article is that the automation of a manual invoice-matching processes is Hammer's primary BPR example. Hammer's paper applies directly to the invoice-matching problem in VAT.

Hammer tells the story of Ford. In the 1980s Ford dedicated 500 employees in its accounts payable department to an invoice-matching function. The company believed that automation — that is, faster computers combined with more efficient and effective programming — would allow faster matching. It expected to achieve a headcount reduction of 20 percent (down to 400 employees) in the team. But when Ford saw that Mazda had only committed five employees to the same invoice-matching function, the company scrapped its automation plans. Radical change was necessary, not just the automation of existing processes.

Ford applied 1980s BPR to commercial invoice matching. It didn't just automate existing processes, it rethought the invoice-matching function, opted for radical change, and went to an online database. Ford called it "invoiceless processing":

Ford has achieved a 75 percent reduction in head count, not the 20 percent it would have gotten with a conventional program. And since there are no discrepancies between the financial record and the physical record, material control is simpler and financial information is more accurate.16

The remaining articles in this series will examine two groups of countries and then consider the questions that those comparisons

<sup>&</sup>lt;sup>15</sup>*Id*. <sup>16</sup>Hammer, supra note 2.

raise for Afghanistan. The first group of countries (South Korea, China, and India) seem to have followed Das-Gupta and Gang — that is, they applied faster computer technology to previously established processes. The second group of countries (Fiji, Samoa, and the Kingdom of Saudi Arabia) seem to have listened to Hammer and Davenport — that is, they tried to break free from the inertia of old processes by rethinking and reengineering the business process of matching invoices.

Afghanistan faces a choice.

### taxnotes



# Tax Notes goes Global.

Get the best of both worlds with *Tax Notes Today Global*, combining our stellar U.S. domestic and international tax news and analysis with a laser-sharp focus on cross-border taxation.

info.taxnotes.com/global

The world of tax
- now available daily.