Capgemini Consulting

# Digital – Blue Skies or a Perfect Storm for the Taxman?

## Our Take on the Impact of Digital Technologies on Tax and Welfare Fraud

# Digital Technologies are Chipping Away at Traditional Tax and Welfare Fraud...

## Fraud is Big Business

The numbers surrounding tax fraud have always been significant. For instance, in the US, tax evasion resulted in revenue loss of over $300 billion during 2010[1]. In the UK, the tax gap amounted to £35 billion in between 2012 and 2013[2]. The EU is estimated to have lost over €193 billion in Value-Added Tax (VAT) revenues due to non-compliance or non-collection[3]. Such large numbers have traditionally kept Government tax and welfare authorities on their toes in the course of time. Authorities have been engaged in a constant battle with fraudsters.

> *In the US, tax evasion resulted in revenue loss of over $300 billion during 2010.*

## Digital Technologies are Helping Tax Authorities Gain New Insights

The advent of digital technologies is helping tax authorities have a slow, but steady, impact on traditional fraud. Data analytics techniques help classify patterns and identify outliers that could indicate fraud (see insert on Her Majesty's Revenue and Customs in the UK). Analytics techniques are used to analyze extensive data such as income, tax paid and asset ownership to spot fraudsters. For instance, in Italy, tax authorities are using a tool called 'Redditometro' or income meter to identify people living above their stated means. The tool looks at over 100 items of spending across several categories, including luxury goods, gymnasium memberships and pay-TV subscriptions to identify if the expenditures are proportionate to the individual's income. If there are discrepancies, the authorities start investigating the identified case[4].

Further, 'social network analysis' or 'link analysis' helps build mathematical models to relate different entities and score their statistical significance for fraud. It is clubbed with other analytics techniques such as predictive modeling and anomaly detection to detect collusive behavior for fraud. For instance, the Los Angeles County implemented an analytics solution, including social network analysis, to combat fraud related to childcare services (see insert).

> *Tax authorities are analyzing extensive data to spot fraudsters.*

### Closing in on Tax Evasion through Data Analytics in the UK – HMRC's Approach

In the UK, the tax gap amounted to £35 billion in 2012. The UK government has invested close to £1 billion so far to tackle tax avoidance, evasion and fraud. In order to achieve this, HMRC used a multipronged approach of taking advantage of technology and analytical techniques. It launched new advertising campaigns, increased the size of its teams dedicated to the fraud and error group, and partnered with private sector experts to overcome tax fraud. HMRC is also incorporating and sharing new data from other countries, from the private sector and from across various government bodies, which allows for more transparency and helps spot the connections between tax evaders' income, wealth and assets.

On the technology front, HMRC has introduced a data warehousing and analytics system called "Connect", at a cost of £45 million. Connect allows HMRC to collate, sift and apply analytics on various data points such as property purchases, tax returns, loans, bank accounts and employment data to identify assets, spot and track suspicious financial transactions and highlight the connections that identify those trying to hide their income and wealth in order to evade tax. HMRC's technology-driven initiative to close-in on tax evasion and fraud delivered almost £2 billion in additional revenues during 2011-12 and is estimated to deliver £22 billion a year in extra tax revenues by 2014-15. It also resulted in over 400 criminal convictions during 2011-12.

Source: Financial Times, "Ten ways HMRC checks if you are cheating", November 2012; HMRC, "Closing in on Tax Evasion-HMRC's Approach", December 2012

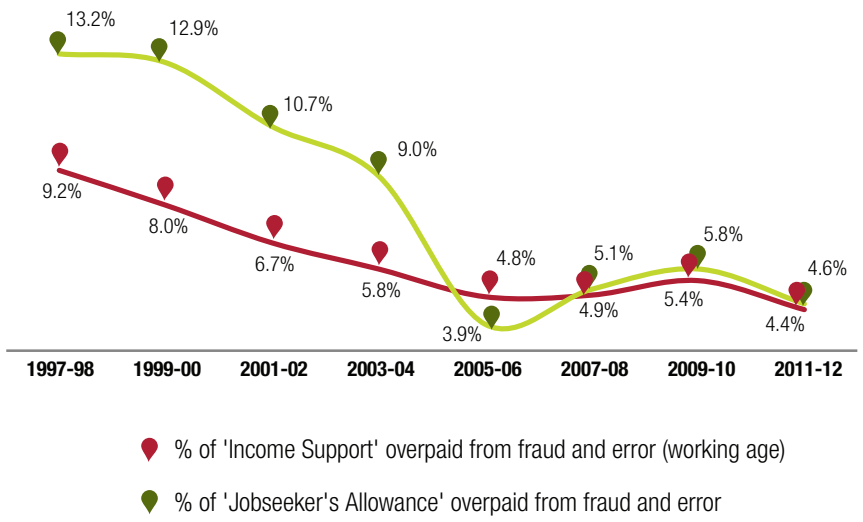
## Digital Technologies are Contributing to a Decline in Traditional Fraud

The increasing usage of digital technologies is helping authorities have a direct impact on losses from fraud and error. There is also growing collaboration and tax information sharing through digital platforms between public authorities globally in order to hone in on cross-border tax evaders.

As a result of these initiatives, overall tax and welfare fraud has reduced in many countries. For instance, VAT gap, a difference between the theoretical total VAT liability (estimated using National Accounts data) and actual cash receipts, in the UK fell from 15.7% in 2002 to 9.5% in 2012[5]. Moreover, the percentage of fraudulent income support over-payments decreased from 9.2% during 1997-98 to 4.4% during 2011-12, while fraudulent jobseeker allowance payments reduced from 13.2% to 4.6% during the same period (see Figure 1).

> *"The UK tax authorities' Big Data solution to combat fraud delivered £2bn in additional revenues during 2011-2012."*

**Figure 1: Percentage of Income Support and Jobseeker's Allowance Overpaid in the UK Due to Fraud and Error**




*Source: DWP, "Fraud and Error in Income Support and Jobseeker's Allowance", March 2002, May 2013*

### Data Mining and Social Network Analytics for Fraud Detection – Los Angeles County's Best Practice Approach

Los Angeles (LA) County's welfare program, providing temporary financial assistance to families with minor children and income below state limits, was facing increasing fraud from participants and child care providers.

In order to detect and prevent fraud, LA County used a data mining service, the first fraud detection system implemented by a local government in the US. This was integrated with predictive models, social network analysis software and business intelligence tools to detect and prevent fraud in public assistance programs. Fraud risk scores were developed to decrease the number of false positive cases assigned to investigators.

Ten months since its launch, the system has produced 197 additional referrals for child care fraud investigations and also detected two conspiring groups consisting of 16 cases. Benefits from the project were calculated across three areas, totalling $6.8 million: new fraud referrals of $2.2 million; early fraud detection of $1.6 million; and increasing program integrity and efficiency of $3 million. The accuracy rate of fraud rings identified by the social network analysis solution was calculated with a reliability of 85 percent.

Source: Los Angeles County, "Data Mining Solution for Child Care Welfare Fraud – Quality and Productivity Commission", 2012

> *Digital technologies have brought about good news. At the same time they have also enabled the rise of a new set of frauds.*

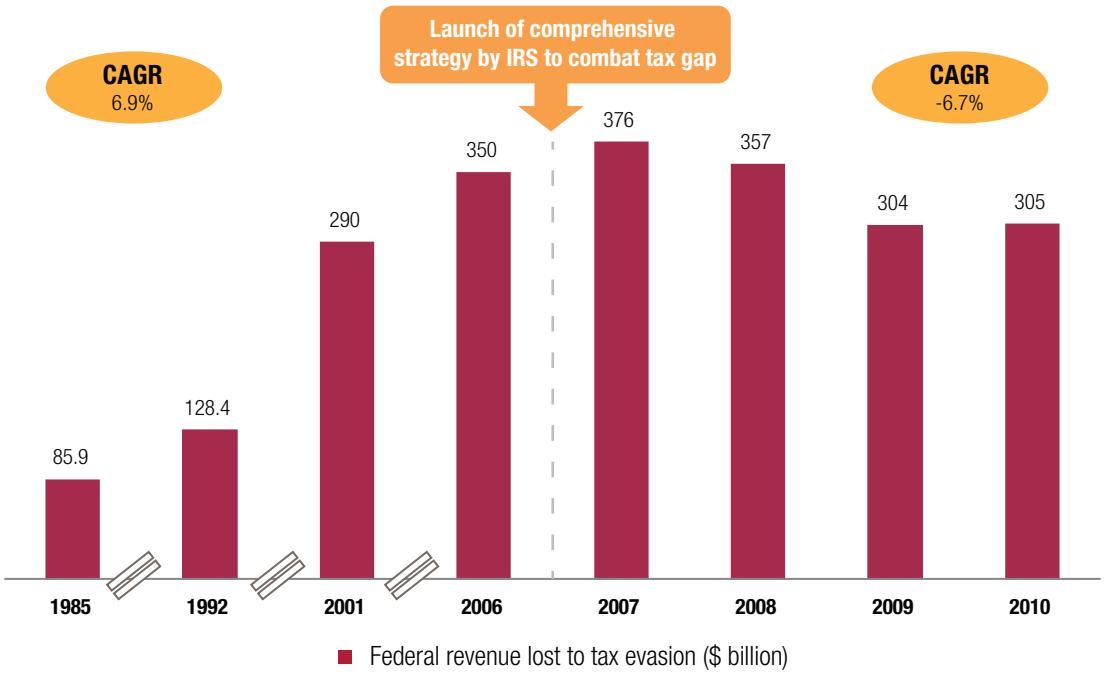
Similarly, HMRC in the UK realized significant achievements in combating tax fraud. Through its compliance operations, during 2003-04 HMRC intervened in over 1,800 incorrect claims where a false or fraudulent tax credits claim was suspected. In the following years, this number increased to 17,000 (2004-05) and 100,000 (2005-06)[6]. This active approach led to a reduction in overall fraud and error in tax credit entitlement from 9.7% in 2004 to 7.8% in 2007 and this further decreased to 7.3% in 2012[7].

In the same context, during 2006 the US Treasury Department came out with a comprehensive strategy for addressing the tax gap. This included measures such as implementing the 'Modernized electronic Filing' (MeF) platform for real-time processing of tax returns and an automated system to identify discrepancies in returns[8]. Consequently, tax evasion is estimated to have declined by nearly 20% during 2007-2010 (see Figure 2).

Digital technologies have brought in good news to tax and welfare authorities. At the same time they have also enabled the rise of a new set of fraud types.

> *Tax evasion in the US is estimated to have declined by nearly 20% during 2007-2010.*

**Figure 2: Federal Revenue Lost to Tax Evasion in the US ($ billion, 1985-2010)**




*Source: US GAO, "Analyzing the Nature of the Income Tax Gap", January 1997; Demos.org, "Tax evasion", 2011*

# ...However, Digital is also Sowing the Seeds for New Frauds

## Digital Creates New Opportunities to Defraud Authorities

Digital technologies are also enabling new types of fraud. The growing prevalence of digital data, sophisticated spyware, phishing software and online scams allow criminals to industrialize fraud, making it harder to detect.

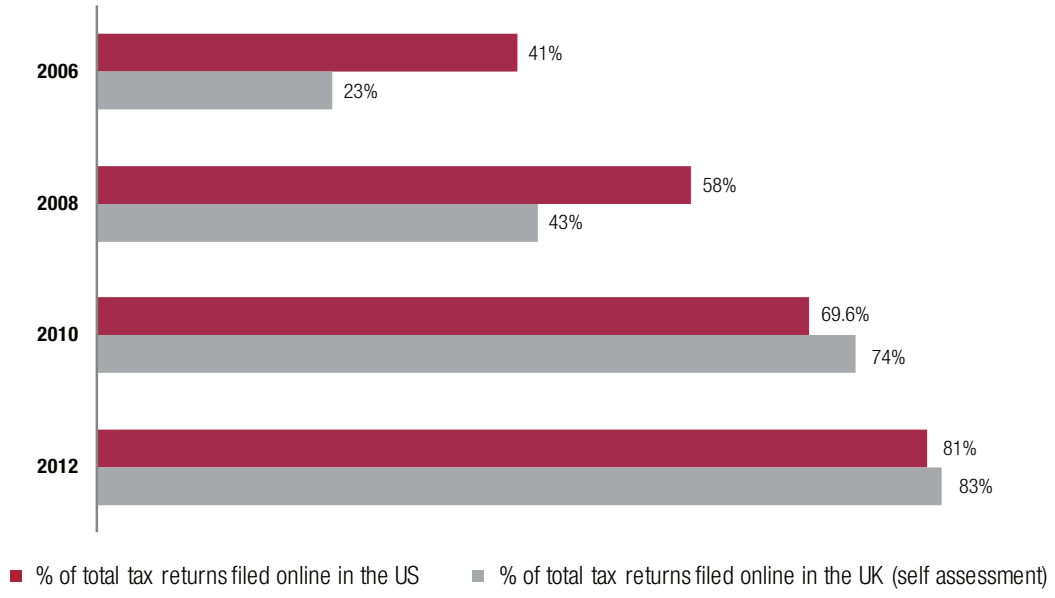
For instance, the growth in digital transactions such as e-banking, e-commerce and online public service payments presents an opportunity for cybercriminals to exploit data trails and digitally stored user information. Similarly, increasing focus on electronic tax filing and associated refund claims also creates an opportunity for tax fraud. The proportion of personal income tax returns filed online (out of total personal income tax returns) in the US increased from 41% to 81% during 2006-12, while it grew from 23% to 83% for the same period in the UK (see Figure 3). Moreover, public sector online databases are also susceptible to intrusion by cybercriminals.

The advent of the Internet also allows for easy creation of shell companies – firms which exist on paper only, with no real employees or offices, possibly in tax havens. These then become the favored vehicle for tax evaders and money launderers as they are easy to set up. These companies can be set up online, sometimes in less than 10 minutes with just an Internet connection and credit card.

These are just two new opportunity areas for digital fraud. However, for tax authorities, the bigger challenge is that consequently, there are several new types of frauds that, have come up, aided by a proliferation of public data and the ease of transmitting and intercepting digital information.

> *"Increasing focus on electronic tax filing creates an opportunity for tax fraud."*

**Figure 3: Growth in E-Filing of Tax Returns in the US and the UK**




*Source: IRS Data Book, 2006-2012; HMRC's online filing figures for self assessment, 2006-12.*

## Digitization Fuels Growth of New Types of Frauds

New tax and benefit fraud types include fraud related to identity theft, zapping, online payroll processing, VAT carousel and digital currencies.

> *In 2012, tax loss due to identity theft was estimated at $11 billion in the US.*

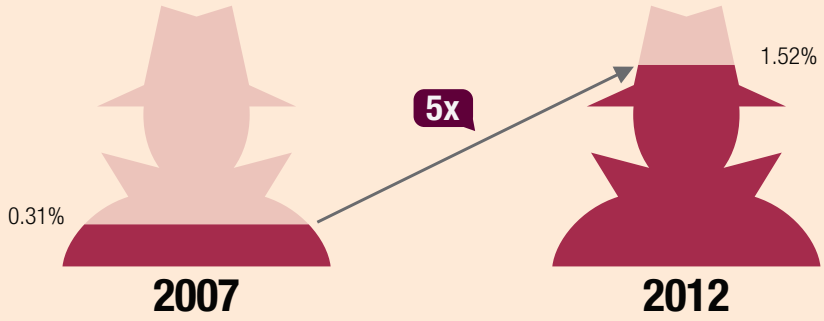
### Growing Incidence of Identity Theft is Driving Tax Refund Fraud

Access to extensive personal data through electronic means has led to a rapid rise in tax fraud through identity theft. Fraudsters, masquerading as authorities, send out emails that request social security numbers or other personal information in order to process tax refunds. Once the user provides this information, it is used to file and claim fraudulent tax returns or even modify bank routing details for tax refunds. Personal information stored with government agencies and banks can also be targeted by hackers to commit identity theft tax fraud (see insert). In 2012, tax loss due to identity theft was estimated at $11 billion in the US and $1.8 billion in the EU (see Figure 4).

### Under-Reporting Income through Zapping Helps Evade Sales and Income Tax

Zappers are programs that automatically and remotely skim cash from electronic cash registers (ECRs) or point of sales (POS) systems, which are then used by businesses to under-report earnings, evade taxes or even launder money. Businesses such as restaurants, convenience stores and gas stations that record significant cash sales with ECRs are most susceptible to zappers.

### Identity Theft is on the Rise with US Internal Revenue Services' (IRS) Move to E-Filing Tax Returns




■ % of identity theft incidents in total personal income tax returns e-filed

Identity theft is the number one tax scam for 2013, and has been increasing in relation to the IRS' growing dependence on electronic tax-filing and the direct-depositing of refunds. E-filing of personal income tax returns in the US grew at a CAGR of 8.5% over 2007 and 2012 period.

The US Tax Administration reported that the IRS failed to identify 1.5 million fraudulent returns related to tax year 2010.

Source: US Senate Committee on Finance, "Tax Fraud and Tax ID Theft: Moving Forward with Solutions", April 2013; The Wall Street Journal, "E-Filing and the Explosion in Tax-Return Fraud", January 2013

> *Zapping helps fraudsters under-report earnings and evade tax by automatically skimming cash from electronic cash registers.*

Once installed, a zapper allows accurate receipts to be issued, but soon after this it eliminates a select number of transactions. The cash associated with these suppressed sales can be skimmed without detection.

Numerous tax fraud zapper cases have been reported in the US. For instance, a dairy in Connecticut skimmed $17 million in receipts and hid the cash in a tax-haven. A restaurant chain in Detroit, Michigan zapped $20 million in cash sales. According to estimates, a third of Canada's restaurants may be evading taxes by using zapper programs and other software to hide their sales. The Canada Revenue Agency has found an estimated $141 million in phantom sales that were deliberately erased in electronic cash registers to avoid taxes[9]. In the US and the EU zapping in restaurants is estimated to have resulted in tax losses of around $2.1 billion and $2.2 billion respectively in 2012 (see Figure 4).

> *A third of Canada's restaurants may be evading taxes by using zapper programs.*

### Online Payroll Processing by Third Parties Leads to Payroll Tax Fraud

Many businesses outsource their payroll services to third-party providers who manage online payroll processing for employees and payroll tax filing. However, some of these providers commit payroll tax fraud by withholding or diverting the client's payroll tax funds. For instance, a payroll services firm in the US paid $19 million in restitution for siphoning off a part of their clients' tax payments and under reporting it to the IRS[10]. Similarly, senior-executives of another payroll services company embezzled nearly $1.3 million from clients and failed to pay $400,000 in taxes. These executives then transferred money from their clients' bank accounts to the company's tax accounts and subsequently onto their own debit cards instead of sending it to the IRS[11]. In 2012, tax loss due to payroll fraud in the US and the EU was estimated to be $5.4 billion and $10.7 billion respectively (see Figure 4).

> *"In 2012, tax loss related to online payroll fraud in the EU was estimated to be $10.7 billion."*

### VAT Carousel Fraud Goes Digital

VAT carousel fraud involves defrauding the government of VAT on the trade of goods and services. It arises when a business makes an intra-community (within EU) purchase without paying VAT, collects VAT on an onward sale, and then "disappears" without remitting the tax.

While VAT carousel fraud traditionally occurred over physical goods such as computer chips, it has now expanded to digital services such as CO2 permits and VOIP services[12]. Online exchanges enable clearing spot transactions for CO2 permits as quickly as fifteen minutes, which acts as a key driver for fraudulent activities[13]. According to the European Police Office, up to 90 percent of the trade in CO2 permits in some countries is fraudulent. A recent study also warns of an emerging threat of this fraud exploiting electricity and gas markets[14]. Tax loss in the EU due to VAT carousel fraud was estimated to be $3.5 billion in 2012 (see Figure 4).

### Digital Currencies Facilitate Tax Evasion

Digital currencies are electronically traded currencies that are not guaranteed by a sovereign state and do not have a 'legal tender'. They act as an alternative to nation-backed currencies and can be exchanged for 'legal' currencies through exchanges. Bitcoin, the largest operational digital currency, had a market capitalization of more than $1 billion in June 2013[15].

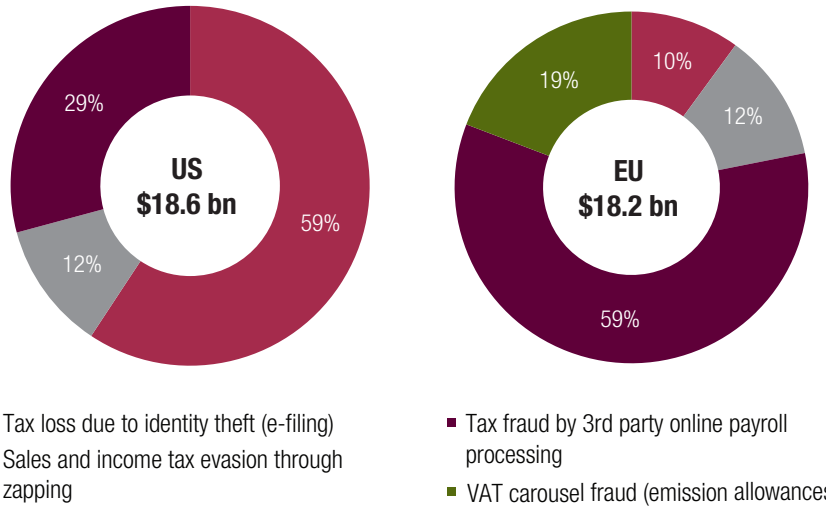
Digital currencies offer higher scope for money laundering and resultant tax evasion. In March 2013, US prosecutors filed a case against Liberty Reserve, alleging that it was running a $6 billion money laundering scheme and operating an unlicensed money transmitting business. Moreover, the Department of Homeland Security restricted the transfer of funds in and out of Mt. Gox, the world's largest Bitcoin exchange, which is based in Japan[16].

Government authorities have so far achieved limited success in preventing the misuse of digital currency due to lack of regulations governing its usage. The overall public revenue loss due to digital currency remains unknown on account of ambiguity in tax treatment and built in privacy of digital currency.

In the next section, we take a look at the actual impact the growth of such digital fraud techniques can have on the US and EU markets in the coming years.

> *"Digital currencies offer higher scope for money laundering and resultant tax evasion."*

**Figure 4: Digital Frauds in the US and the EU ($ billion, 2012)**




*Source: IRS, US Census; National Restaurant Association (US); National Association of Convenience Stores (US); National Small Business Association; Eurostat/OECD Statistics; Capgemini Consulting Analysis*

# Inaction on Digital Fraud Could Cost the US and the EU Nearly $35 Billion Each

## If Left Unchecked, Digital Fraud Will Double in Value by 2020 in the US and the EU

To understand the impact that digital fraud can have on tax authorities in the future, we built a comprehensive forecasting model. We evaluated a wide range of parameters in order to identify the quantum of digital fraud that can hit the US and the EU by 2020 (see insert on our approach on page 10). Specifically, we looked at identity theft, zapping, third-party payroll processing and VAT carousel. The results from our forecast show that if tax authorities continue to rely on existing ways and means of fighting digital fraud, i.e. if they adopt an 'as is' approach, they are in for an uphill battle. In such a scenario, we estimate digital fraud to almost double to over $34 billion in the US and $35 billion in the EU by 2020 from $18.6 billion and $18.2 billion in 2012 respectively.

> *"If left unchecked, digital fraud will double in value by 2020 in the US and the EU."*

Digital fraud in the US and the EU is driven by different factors (see Figure 5). In the case of US, the main driver is tax loss due to identity theft, a consequence of growing numbers of e-filings. ID theft fraud has been a matter of concern for authorities in the US for a while. Indeed, the IRS has described identity theft as the number one tax scam of 2013[17]. Fraudsters typically rely on using a combination of people staying on temporary visas, fake names, prepaid cellphones, disguised computer addresses and fraudulent bank accounts. In a recent case, authorities in the US indicted over 55 people in a bogus scheme that netted $7 million and involved the theft of more than 2,000 identities[18].

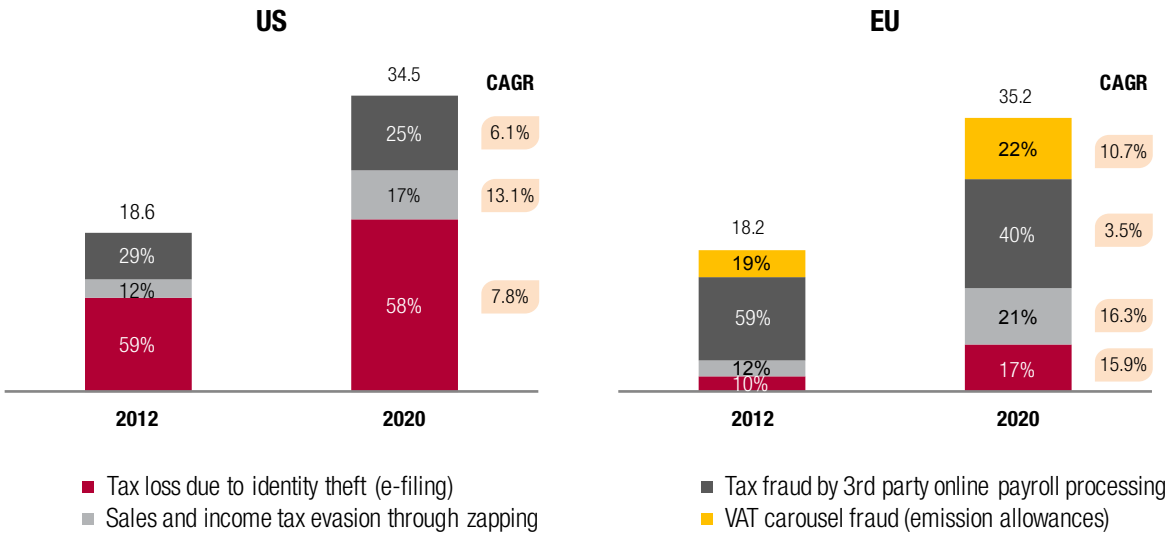
In the case of the EU, tax fraud by third-party online payroll processing firms is the biggest source of digital fraud. This is due to a combination of factors. For instance, the larger employment base in the SME (Small and Medium Enterprise) sector, higher payroll deductions and more propensity to outsource payroll processing in the EU (55%) as compared to the US (40%) make payroll processing an attractive target for fraudsters[19]. These factors together make tax fraud in online payroll processing a key contributor to overall digital fraud in the EU.

Among the other types of fraud, zapping is estimated to grow extremely rapidly, albeit from a smaller base. We forecast tax loss due to zapping to grow by 167% in the US and 235% in the EU. Such growth is driven by an increase in restaurant sales and rising taxes. Restaurant sales in the US and the EU registered 13.3% and 11.2% growth during 2010-12 respectively and is further anticipated to grow steadily over the 2013-20 period[20].

> *"Tax loss due to zapping is estimated to grow by 167% in the US and 235% in the EU."*

VAT carousel fraud in emissions allowances is a fraud category that is exclusive to the EU region. We estimate it will more than double during 2012-2020. This is on the back of an increase in the trade volume as well as an anticipated rise in the price of CO2 emission allowances.

**Figure 5: Breakdown of Forecasted Digital Fraud under 'as is' Scenario (US and EU, 2012-2020)**




*Source: Capgemini Consulting forecasts*

## Such Strong Growth Will Drive a Shift in Fraud Mix

Despite a steady increase in digital fraud, the good news for tax and welfare authorities is that traditional fraud continues to reduce. We expect technological solutions such as using analytics to identify potential fraudsters, to help authorities fight traditional fraud with increased success. However, at the same time, the newer types of fraud will grow much more rapidly than the rate at which traditional fraud is declining. This will result in digital fraud accounting for a greater proportion of overall fraud in the coming years. Our estimates indicate that in an 'as is' scenario, where additional interventions are not made to tackle digital fraud, the overall fraud mix will see significant change. In the US, by 2020, nearly one-sixth of all fraud will be digital in nature. Similarly, in the EU, digital fraud will grow from 5% to nearly 18% of the overall fraud mix (see Figure 6).

For tax and welfare authorities, all is not lost. Digital technologies can also help where they hurt the most.

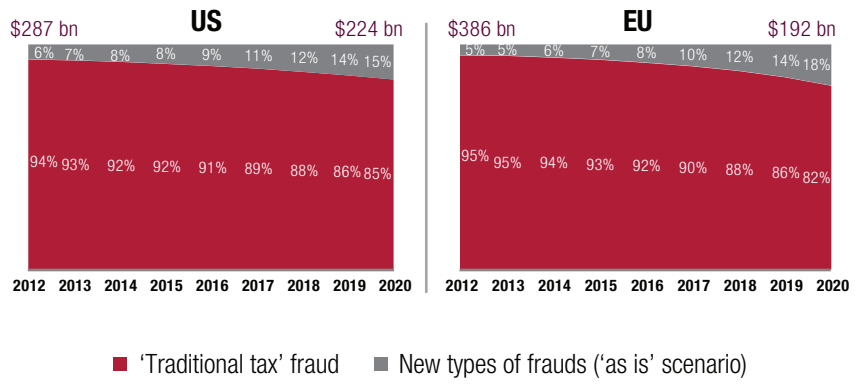
## A Strong Vision Coupled with Digital Interventions Can Sharply Curtail the Growth of Emerging Frauds

Tax and welfare authorities can combat digital fraud by implementing technological solutions. There are two broad approaches that tax authorities can take – an incremental approach and a holistic approach.

In an "incremental approach" tax authorities can deploy multiple discrete solutions to prevent new types of fraud. This will involve launching multiple measures to control specific fraudulent activities in the short to medium term. However, this approach has its challenges. It is reactive by nature and typically lacks a structured governance model around it. These measures, while effective individually, lack the synergies that a coordinated response can achieve. For instance, the US IRS has as many as 21 departments looking at identity theft[21]. We estimate that if tax and welfare authorities in the US and the EU intervene through discrete, incremental solutions during 2012-2020, the growth of digital fraud can be curtailed from 85% to 32% in the US and from 93% to 26% in the EU.

Tax authorities who understand and appreciate the impact that digital fraud can have will adopt a more 'holistic approach'. In this scenario, we believe authorities will undertake comprehensive technological and governance measures in order to detect and prevent digital fraud. Such an approach involves long-term vision, adoption of a clear roadmap and multipronged solutions involving people, processes and technology to combat digital fraud (as explained in greater detail in the next section). Adopting such an approach can help authorities decrease digital fraud by nearly 50% in the US and 41% in the EU during 2012-2020 (see Figure 7).

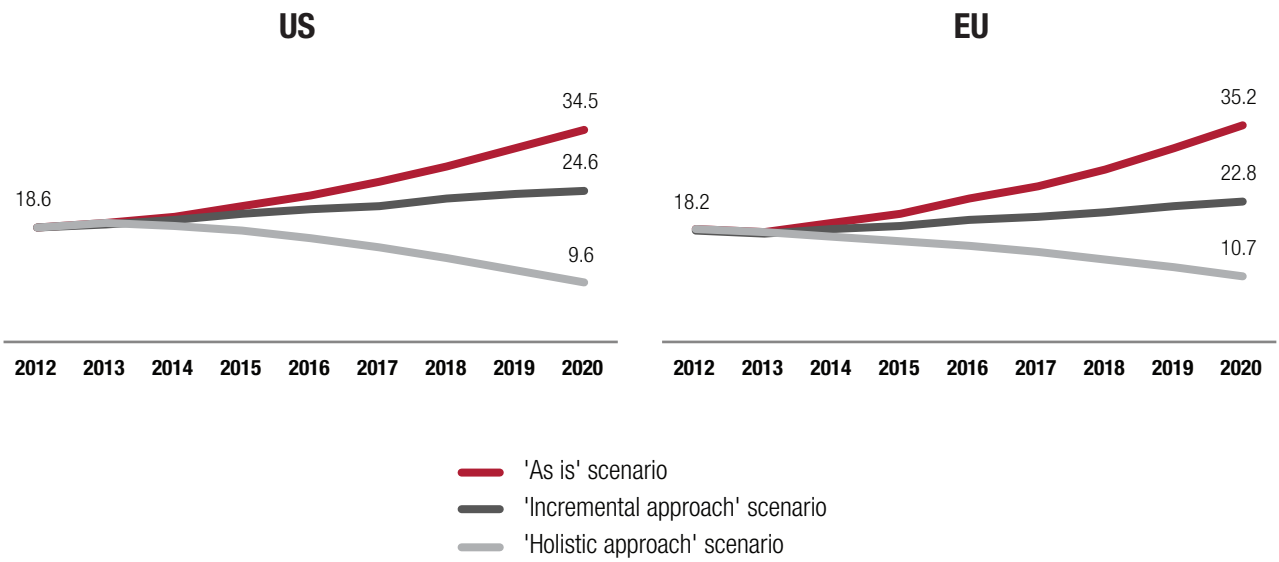
**Figure 6: Projected Trend of Traditional and New Types of Tax Frauds (US and EU)**




*Source: Capgemini Consulting forecasts*

> *"Adopting a holistic approach can help authorities decrease digital fraud by nearly 50% in the US and 41% in the EU."*

**Figure 7: Impact of Digital Solutions in Curtailing Digital Fraud (US and EU, $ billion)**




*Source: Capgemini Consulting forecasts*

## Our Approach to Forecasting Revenue Loss due to Digital Fraud in the US and the EU

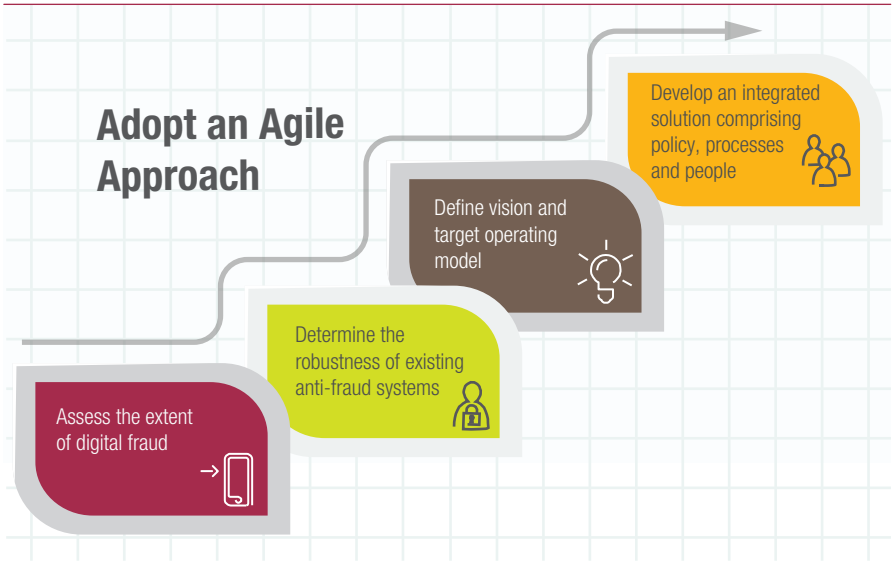
We built a forecasting model to estimate the impact of digital fraud in the US and the EU until 2020 by analyzing four fast growing frauds – identity theft, zapping, third-party online payroll processing and VAT carousel related to emission allowances. Revenue loss to government authorities due to tax related identity theft was estimated using identity theft incidents, tax return e-filing statistics and employment data. Restaurant sales, percentage cash transactions, average income and applicable taxes were considered to forecast sales tax and income tax losses due to zapping. While annual payroll data, standard deductions, percentage of firms outsourcing payroll services and employment data were used to project third-party online payroll processing fraud. VAT carousel fraud was determined using EU specific emissions allowances trade volumes, prices of carbon credits and average VAT rates applicable on carbon trading.

# Tax and Welfare Authorities Need to Act Now To Curb Growth in Digital Fraud

The strong increase in digital tax and welfare fraud calls for multipronged solutions from tax and welfare authorities. As new digital technologies and platforms continue to emerge, so will the types of tax and welfare fraud. This calls for innovative and comprehensive ways to tackle emerging fraud. In this section, we present a roadmap for implementing solutions to counter new types of digital tax and welfare fraud (see Figure 8).

> *"As new digital technologies and platforms continue to emerge, so will the types of tax and welfare fraud."*

**Figure 8: Roadmap to Combat Digital Tax and Welfare Fraud**




*Source: Capgemini Consulting*

## Assess the Extent of Digital Fraud

The first step in combating new types of digital tax and welfare fraud is to identify them and assess their spread and financial impact. One of the ways in which this can be done is by running one or several pilot projects to analyze the incidence of fraud in a sample population. For instance, the Canada Revenue Agency ran a three-year pilot project that analyzed electronic sales data at 424 establishments to understand the extent of zapping. It discovered at least 143 cases of suspected fraud, each with an average of $1-million in phantom sales[22]. This led to a crack down on zappers, including installation of special recorders to document every sale punched into cash registers.

## Determine the Robustness of Existing Anti-Fraud Systems

Tax and welfare authorities need to assess the efficacy of existing anti-fraud systems in identifying and preventing digital tax and welfare frauds. This can be done through regular audits, which will help reveal loopholes and missing capabilities. For instance, the IRS uses a series of filters to flag and stop potentially fraudulent returns (see insert). However, an audit revealed that a majority of the tax returns that were flagged as 'unpostable' (illegitimate) by the IRS, due to inability to clear identity theft screening filters or missing online identification numbers (IPPINs[a]), were eventually deemed legitimate. The audit identified accuracy of the screening filters as the key missing capability in this case[23].

Once missing capabilities are determined, they should be prioritized and included in existing or new anti-fraud systems. One way to prioritize these capabilities is to create a heat-map that reflects the potential amount of tax fraud averted as a result of adding different capabilities. The capability mix that leads to maximum savings can then be prioritized over others, subject to factors such as cost and compatibility with existing systems.

> *"Tax and welfare authorities need to assess the efficacy of existing anti-fraud solutions in preventing digital fraud."*

a Identity Protection Personal Identification Numbers (IPPINs) are issued to victims of identity theft tax fraud by the IRS for additional protection while e-filing tax returns

## Define Vision and Target Operating Model

Tax and welfare authorities need to clearly define their vision and target operating model for combating digital fraud. For instance, in the US, the IRS defined a vision of implementing a "Real Time Tax System" that would allow matching of data on tax returns with data in IRS's records at the time the tax return is submitted for filing[24]. Similarly, tax authorities should have clarity about the short-term and long-term benefits expected from the solution that they wish to deploy to counter fraud. At the same time, tax authorities should bear in mind that addressing growing digital fraud is not a technological battle alone. Technology solutions should be closely driven in tandem with business efforts.

> *"A successful solution for countering digital fraud requires an integrated approach covering policies, processes, people and technology."*

### Key Measures taken by IRS to Combat Tax-Related Identity Theft

The IRS has taken multiple measures to combat ID theft. It uses identity theft screening filters that spot fraudulent tax returns before refunds are issued and adjusts these filters periodically. The use of these filters enabled IRS to stop issuance of nearly $2.2 billion in fraudulent tax refunds in 2012. The IRS also has an 'external leads' program, wherein private businesses alert it of suspicious transactions. IRS then investigates the taxpayers involved in these transactions and recoups the funds from financial institutions. The 'external leads' program has helped recover more than $293 million from 122,000 accounts in 2013.

Another initiative by IRS to combat ID theft tax fraud is the use of online tools to facilitate research in ID theft cases. It has adopted Integrated Automated Technologies (IAT), a software suite that allows employees to conduct research, adjust accounts and send letters to affected taxpayers. The IRS has also set up a dedicated 'Identity Theft Clearinghouse' to accept tax fraud-related identity theft leads from its Criminal Investigation field offices. The Clearinghouse develops each lead and supports ongoing criminal investigations involving identity theft.

It also provides additional protection to victims of identity theft tax fraud. These taxpayers are issued 'Identity Protection Personal Identification Numbers (IPPIN) which adds an additional layer of security in e-filing taxes. For the 2013 filing season, IRS issued more than 700,000 IPPINs.

The IRS has reorganized to establish an 'Identity Theft Program Specialized Group' in all business units where employees are assigned specifically to work the identity theft portion of the case. It has also implemented new tools such as the Identity Theft Case Building Guide and the Identity Theft Tracking Indicator Assistant tool to help telephone assistors in resolving identity theft cases.

These efforts helped the IRS protect $20 billion of fraudulent refunds in 2012, including those related to identity theft, compared with $14 billion in 2011.

Source: IRS Identity Theft Advisory Council, Identity Theft Status Update, June 2013; TIGTA US Senate, 'Tax Related Identity Theft: An Epidemic Facing Seniors and Taxpayers', April 2013

## Develop an Integrated Solution Comprising Policy, Processes, People and Technology

A successful solution for countering emerging types of tax and welfare frauds requires an integrated approach covering policies, processes, people and technology. Policies including legislation and guidelines need to be drafted to discourage fraudulent behavior. For instance, the State of Washington recently enacted laws to thwart zapping[25]. Implementation of policy also needs robust processes that are difficult to bypass. For instance, Swedish law now mandates that POS systems must meet strict technical requirements and be connected to a control unit that produces a digital signature based on the content of the receipt[26].

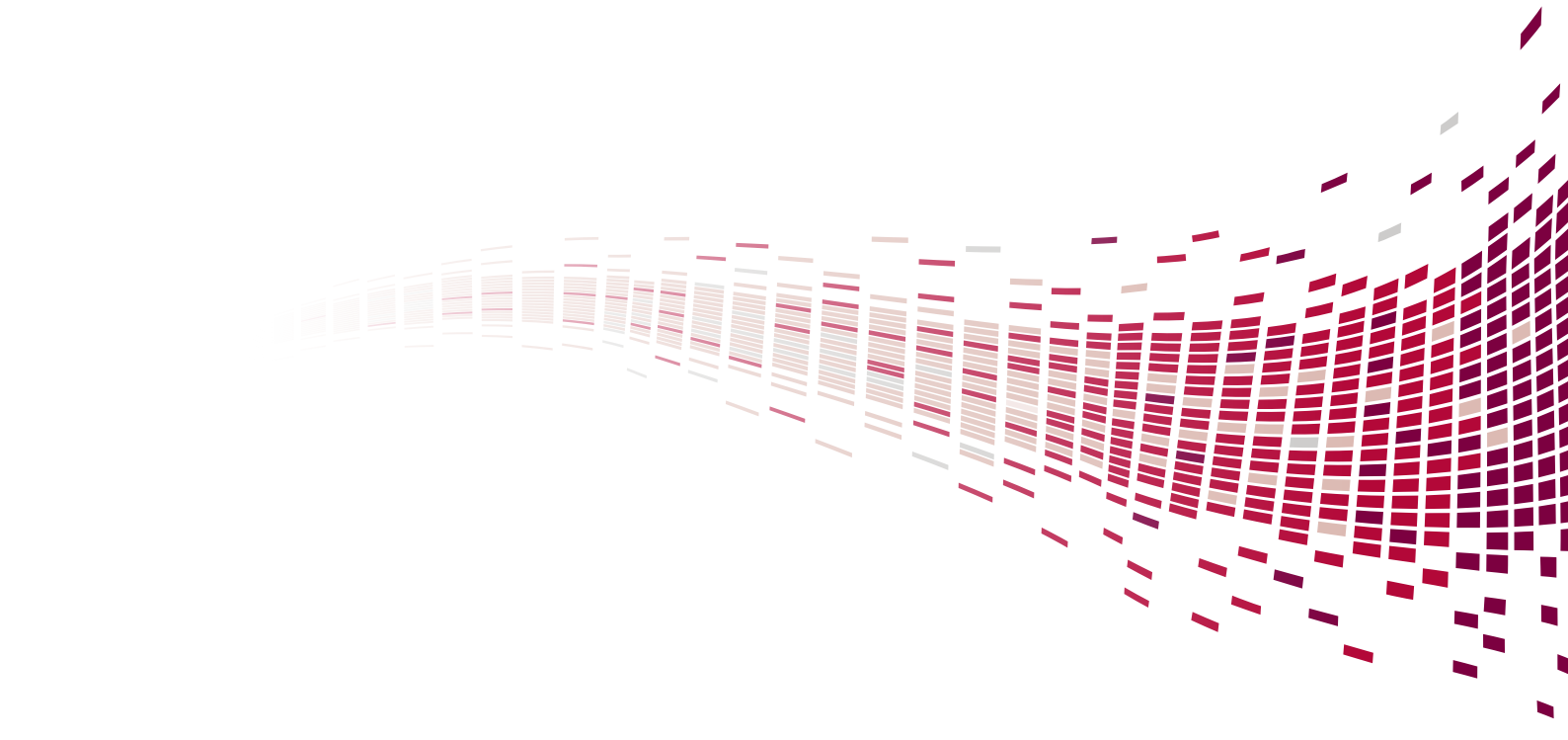
While polices and processes play key roles in the fight against tax and welfare fraud, people play the most significant role in this battle. Employees need to be sensitized about new ways of tackling fraud. Identifying internal fraud and collusion with external fraudsters is another area where people play a critical role. Similarly, taxpayers and beneficiaries of welfare schemes need to be educated on the risks of fraud such as identity thefts and how they can take steps to secure their personal data. Tax authorities should also ensure they stay ahead of latest technologies. They need to do this by constantly refreshing their understanding of new technological platforms that can be used to enhance citizen experience, while keeping off fraudsters.

## Adopt an Agile Approach

Countering fraud and evasion calls for an agile implementation approach. It involves running pilot projects to test aspects of the potential solution. This will help prioritize the rollout of new capabilities and control costs. Pilot projects also offer valuable lessons that can be used to improve the final solution implemented across the organization. An effective feedback mechanism needs to be established in order to keep pace with evolving patterns of fraud, including dynamic models that evolve in real time, and prediction and identification of new techniques of committing fraud.

Revenue loss through digital tax and welfare fraud is a significant concern for countries that are currently struggling to rein in their fiscal deficit. While it is difficult to combat digital fraud with traditional measures, nevertheless, it can be effectively contained through the implementation of robust digital capabilities that can identify and thwart emerging fraud. The efficacy of such systems has already been established, with ROI as high as 50x in some instances[27]. In the US, the Centers for Medicare and Medicaid Services implemented new anti-fraud tools using predictive analytics that prevented or identified an estimated $115.4 million in payments. The program achieved positive ROI in its first year of operation, saving an estimated $3 for every $1 spent[28]. Government authorities should leverage the potential of innovative digital solutions to increase tax compliance, reduce welfare fraud and ensure better services for citizens.

While it is true that traditional fraud is on the decrease, however, as we have shown, that isn't exactly enough reason for tax and welfare authorities to relax. As digital technologies keep growing in complexity and capability, fraudsters will continue to get bolder. They will try newer ways of circumventing established protocols. Unless government authorities stay one step ahead of fraudsters in the usage and understanding of emerging digital technologies, the blue skies that digital brings can very quickly vanish and turn into a perfect storm.



## References


1 Demos.org, “Tax evasion”, 2011

2 HMRC, “Measuring Tax Gaps 2013 Edition”, October 2013

3 European Commission Report, “Study to quantify and analyse the VAT Gap in the EU-27 Member States”, July 2013

4 Enterprise Efficiency, “Italian Tax Authorities Automating Fraud Detection”, May 2013

5 HMRC, “Second Estimate of the VAT Gap for 2011-12”, March 2013; HMRC’s Estimates of the UK VAT Gap, 2005

6 Centre For Tax Policy And Administration OECD, “Report On Identity Fraud: Tax Evasion And Money Laundering”, 2006

7 HMRC, “Child and Working Tax Credits – Error and Fraud Statistics 2011-12”, 2013

8 US Department of the Treasury, “Update on Reducing the Federal Tax Gap “, July 2009

9 The Globe and Mail, “Taxman finds rampant restaurant fraud”, September 2012

10 The Baltimore Sun, “Mikulski to propose bill in wake of alleged Harford payroll firm tax fraud”, April 2013

11 The United States Attorney’s Office, District of New Jersey, “Two former executives of first priority pay plead guilty to conspiracy to commit wire fraud and tax fraud”, October 2011

12 International VAT Monitor, “Technology Can Solve MTIC Fraud- VLN, RTvat, D-VAT certification”, June 2011

13 BU School of Law, “CO2 MTIC Fraud- Technologically Exploiting EU VAT”, 2010

14 Europol, “EU Serious and Organized Crime Threat Assessment”, 2013

15 Coinmarketcap.com, “Crypto-Currency Market Capitalizations”, June 2013

16 PC World, “Mt. Gox accused of violating US money transfer regulations”, May 2013

17 IRS, “IRS Releases the Dirty Dozen Tax Scams for 2013”, March 2013

18 Federal Bureau of Investigation, “More Than 50 People Indicted in Massive Fraud Ring”, September 2013

19 National Small Business Association, “2013 Small Business Taxation Survey”, 2013; ADP, “Payroll Outsourcing in Europe”, July 2008

20 National Restaurant Association, US; Eurostat

21 IRS, “Annual Report to Congress”, December 2012

22 The Globe and Mail, “Taxman Finds Rampant Restaurant Fraud”, August 2011

23 US House of Representatives, Statement of National Taxpayer Advocate on Identity Theft Related Tax Fraud before the Committee on Oversight and Government Reform, August 2013

24 American Bankers Association, “IRS Real Time Tax System Initiative”, January 2012

25 Newsroom Department of Revenue, Washington State, “Government Signs Bill to Zap Zappers”, 2013

26 OECD, “Electronic Sales Suppression: A Threat to Tax Revenues”, 2013

27 Mynewsdesk.com, “Record £220m Haul From Wealthy Taxpayers”, April 2012

28 Centers for Medicare & Medicaid Services, “Report to Congress Fraud Prevention System First Implementation Year,” 2012

## Authors


**Andrew Lennox**
Vice President, UK
*andrew.lennox@capgemini.com*

**Olivier Djololian**
Principal, UK
*olivier.djololian@capgemini.com*

**Digital Transformation Research Institute**
*dtri.in@capgemini.com*

**Jerome Buvat**
Head of Digital Transformation Research Institute, UK
*jerome.buvat@capgemini.com*

**Vishal Clerk**
Senior Consultant, Digital Transformation Research Institute, India
*vishal.clerk@capgemini.com*



*The authors would also like to acknowledge the contributions of **Amit Srivastava** and **Subrahmanyam KVJ** from the **Digital Transformation Research Institute,** and **Tripti Sethi** from the Capgemini Consulting India Digital Transformation team.*


## For more information contact:


Australia
**Shelley Oldham**
*shelley.oldham@capgemini.com*

Germany
**Tom Gensicke**
*tom.gensicke@capgemini.com*

UK
**Richard Kershaw**
*richard.kershaw@capgemini.com*

Belgium
**Pierre Lorquet**
*pierre.lorquet@capgemini.com*

Netherlands
**Marleen van Amersfoort**
*marleen.van.amersfoort@capgemini.com*

France
**Ludovic De Lamazière**
*ludovic.delamaziere@capgemini.com*

Sweden
**Henrik Poppius**
*henrik.poppius@capgemini.com*


Capgemini Consulting

Capgemini Consulting is the global strategy and transformation consulting organization of the Capgemini Group, specializing in advising and supporting enterprises in significant transformation, from innovative strategy to execution and with an unstinting focus on results. With the new digital economy creating significant disruptions and opportunities, our global team of over 3,600 talented individuals work with leading companies and governments to master Digital Transformation, drawing on our understanding of the digital economy and our leadership in business transformation and organizational change.

Find out more at:
http://www.capgemini-consulting.com/

*Rightshore® is a trademark belonging to Capgemini*

### About Capgemini and the Collaborative Business Experience

With more than 125,000 people in 44 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2012 global revenues of EUR 10.3 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fi t their needs and drive the results they want. A deeply multicultural organisation, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at www.uk.capgemini.com


*Capgemini Consulting is the strategy and transformation consulting brand of Capgemini Group. The information contained in this document is proprietary.*
*© 2013 Capgemini. All rights reserved.*