Capgemini Consulting

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Taming Tax Fraud's New Digital Frontier: What Can Tax Authorities Do to Take On Fraudsters and Win

Executive Summary

If there's one major area of criminal activity that is renowned for big numbers, it is fraud. In the US, the Internal Revenue Services (IRS) estimates that tax evasion cost the federal government, on average, $458 billion per year between 2008 and 2010[1]. The UK government estimates tax fraud costs £16bn a year[2]. The VAT gap in EU in 2014 alone is estimated to be as much as €160 Billion[3].

Innovative new technologies have been very efficient in combating traditional fraud. In Belgium, for example, the Federal Public Service Finance department uses multiple analytical techniques to detect VAT fraud, which has reduced losses by 98%, from as much as 1.1 billion euros in 2002 to just under 19 million euros in 2012. The tool allows proactive detection of companies at risk and enables the tax authorities to take appropriate safeguards[4].

However, digital technologies are a double-edged sword. These smart technologies are also giving rise to new types of digital tax fraud:

1. The increase in the number of e-filings of tax returns across geographies is driving new types of frauds using identity theft as the basis;
2. Another type of fraud taking shape is Zapping – using software programs to automatically skim cash from electronic cash registers (ECR) or point of sale systems;
3. Similarly, the growing usage of third-party payroll processors is opening up a whole new avenue of fraud where unscrupulous processors siphon off taxes due to the state.

Capgemini's analysis of these new digital tax frauds shows that inaction is not an option for tax authorities. We have modelled the evolution of tax fraud, taking into account new incidences of fraud enabled by digital technologies. Our findings are sobering for tax authorities. In a scenario where tax authorities continue to fight new tax fraud with conventional tools, we estimate digital tax fraud in the US will rise from $32 billion to $49 billion by 2020. Similarly, in the EU, we estimate it will surge from $15 billion to $25 billion. And of course the value of fraud is in effect lost revenue to the state and the tax payer. In continued times of limited GDP growth and economic restraint, governments cannot ignore this outflow to the unseen 'dark' economy.

To combat this staggering scale of fraud, conventional methods that involve outdated systems and heavy manual inspection of suspicious fraud are too slow for the digital age. Add to that an environment where budgets are squeezed, many agencies are left, figuratively, bringing a knife to a gun fight. And thirdly, with the increasing pervasiveness of digital technology, digital tax fraud will continue to expand into new areas.

To effectively combat this threat, tax authorities must move away from an incremental, piecemeal approach to fraud, but must adopt a much more comprehensive transformative line of attack with a long-term vision, roadmap and multi-faceted solutions involving people, processes and technology. An example of this approach is taking place in Australia. The "Reinventing the Australian Tax Office" (ATO) program aims to build on effective use of digital technology. In addition to building advanced analytics capabilities, the ATO is taking the necessary cultural and organizational steps to equip itself for the digital age[5].

Analytics is at the heart of this approach and is proving to be a powerful weapon in the fight against digital fraud. We believe that tax authorities must take an exhaustive, multi-step approach to harness the full potential of analytics, ranging from social network analysis, anomaly detection, through to upstream predictive analytics.

Capgemini provides a view on a potential roadmap for building the appropriate analytics capabilities and embedding them into the organization. Key steps of this roadmap include:

- Assessing the extent of digital fraud
- Determining the robustness of existing anti-fraud systems
- Defining a vision and target operating model
- Developing an integrated solution comprising policy, processes, people and technology
- Adopting an agile implementation approach

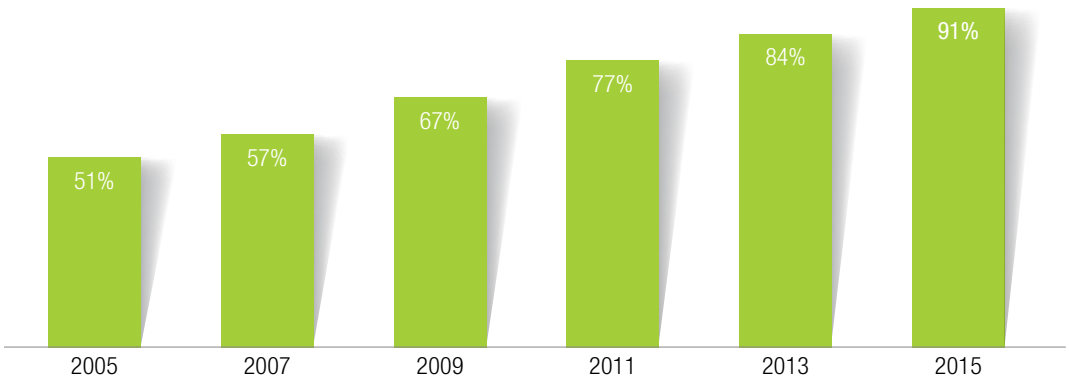
In our view, unless government authorities stay one step ahead of the fraudsters on the digital curve, their opponents could seize the upper hand in the digital tax war.

Digital Tax Fraud is Getting Out of Hand

The menace of digital tax fraud is now bigger than ever. Tax authorities need to move fast to contain and reverse its spread even as it threatens to get out of control. With the world becoming more connected, the opportunities for the digital tax fraudsters are proliferating. Several factors are driving the potential of tax fraud:

- In the US, the proportion of personal income tax returns filed online has increased steadily (see Figure 1). The increasing ease with which a tax return can be filed makes it easier for scammers to swindle the system as well. For instance, filing a return in the US only takes a name, date of birth and Social Security Number. Owing to frequent consumer data breaches, this kind of information is now easily available to hackers and criminals operating on the 'dark web'. In addition, tax authorities are often unable to reconcile refund claims with authentic data - such as employment information from employers - before processing refunds. This aggravates the problem[6].
- Shell companies are now easier to set up and, in some geographies, much easier to liquidate as well. A firm that exists on paper only, with no real employees or offices, can be set up online, sometimes in less than 10 minutes, with just an Internet connection and credit card. In some geographies, they can also be liquidated as fast as they are set up. In the Netherlands, a company can liquidate itself, as long as it can show that it possesses no assets. Moreover, the process of 'losing' assets itself can mean greater scope for fraud[7].

Figure 1: E-Filing in the US, 2005-2015



Source: IRS releases

- Sophisticated software programs are taking fraud into new areas – for instance point of sale systems in restaurants, or payrolls of large corporations.

Furthermore, increasing volumes of digital data, sophisticated spyware, phishing software and online scams allow criminals to industrialize fraud, making it even harder to detect. A number of areas in particular are proving to be a headache for authorities:

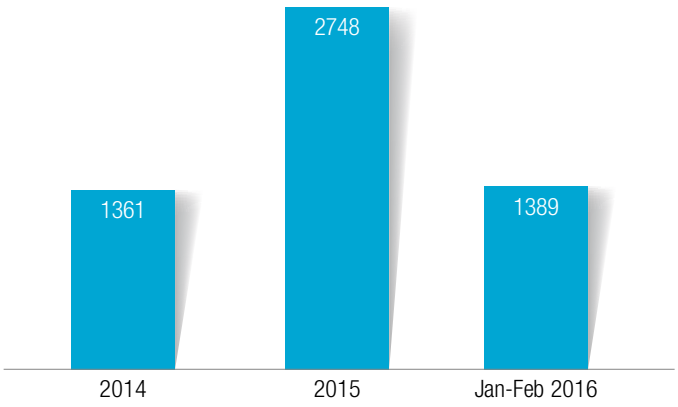
- Identity theft as a means to tax fraud
- Zapping and its impact on revenue declaration
- Third party payroll processing leading to payroll tax fraud

Identity Theft, a Precursor to Tax Fraud, Poses a Major Threat

Identity theft is on the rise globally. For instance, in the UK, the number of victims of identity fraud increased by 57% in 2015. Of these frauds, over 85% were conducted online[8]. In the US, in first six weeks of 2016 alone, the number of reported phishing and malware incidents, designed to steal unsuspecting consumers' sensitive private information, exceeded the total number of incidents in 2014, and quickly reached over half of 2015's total incidents (see Figure 2)[9]. Identity theft complaints to the US Federal Trade Commission rose nearly 50% from 2014 on the back of a steep rise in complaints about identity based tax fraud (see Figure 3)[10].

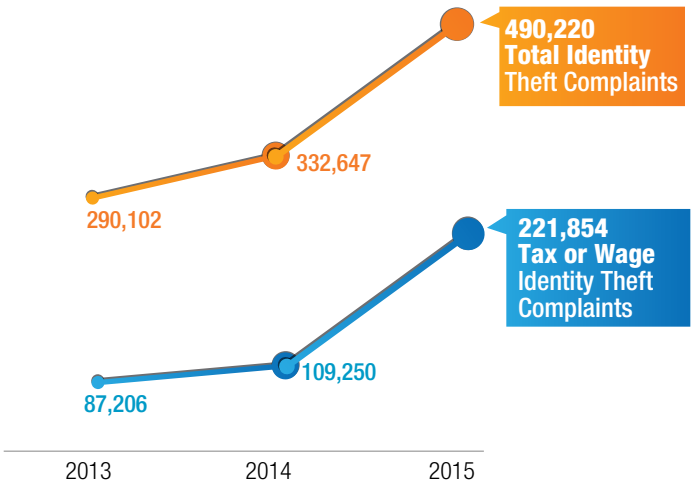
This is a worrying trend for the tax industry as identity theft serves as a precursor to tax fraud. The stolen identity details are then used to deceive the tax system – such as by filing fraudulent returns, making fake refund requests or sending false communication to taxpayers impersonating the IRS, tricking them into paying up (see "The Anatomy of an Identity Theft Tax Fraud").

Figure 2: Reported Phishing and Malware Incidents, 2014-2016 (First six weeks of 2016)



Source: IRS, "Consumers Warned of New Surge in IRS E-mail Schemes during 2016 Tax Season; Tax Industry Also Targeted", February 2016

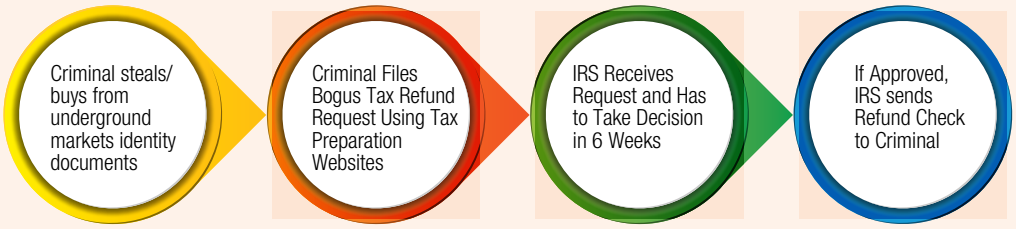
Figure 3: Identity Theft Reported to the US Federal Trade Commission, 2013-2015



Source: Federal Trade Commission, "FTC Releases Annual Summary of Consumer Complaints", March 2016

The Anatomy of an Identity Theft Tax Fraud

The rise of identity fraud is closely tied to how easy it is to perpetrate. The fraud takes advantage of several loopholes in the system. For instance, in the US, the IRS is mandated to decide on a refund request within six weeks of receipt. In practice though, the IRS issues more than 9 out of 10 refunds in less than 21 days[1]. Moreover, the bulk of return fraud happens at the start of the tax season. At this point, most organizations are yet to submit W-2 forms – the statutory forms that show the amount of tax withheld from pay[2]. Taking advantage of these loopholes, criminals can file tax refund requests using identity data that's getting increasingly easy to find, as depicted below:



The time between the filing of a refund request and approval of refund is often less than a week, making this a highly attractive prospect for fraudsters. Moreover, perpetrators can also get the refund paid directly to prepaid cards from mainstream retailers, thereby eliminating the need for the criminal to expose their identity. Once the refund comes back to the card, it can be withdrawn as cash using any ATM and the cards disposed of.

Sources:

1. IRS, "What to Expect for Refunds in 2016", 2016
2. CBS News, "60 Minutes - The Tax Refund Scam", June 2015

Zapping Grows on the Back of Increased Economic Activity

Zappers are programs that automatically skim cash from electronic cash registers (ECRs) or point of sales (POS) systems. This allows a business 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. Once installed in the ECR, a zapper allows accurate receipts to be issued, but soon after this, it eliminates a select number of transactions from being recorded. The cash associated with these suppressed sales can then be skimmed by the business without detection, leading to unlawful tax evasion.

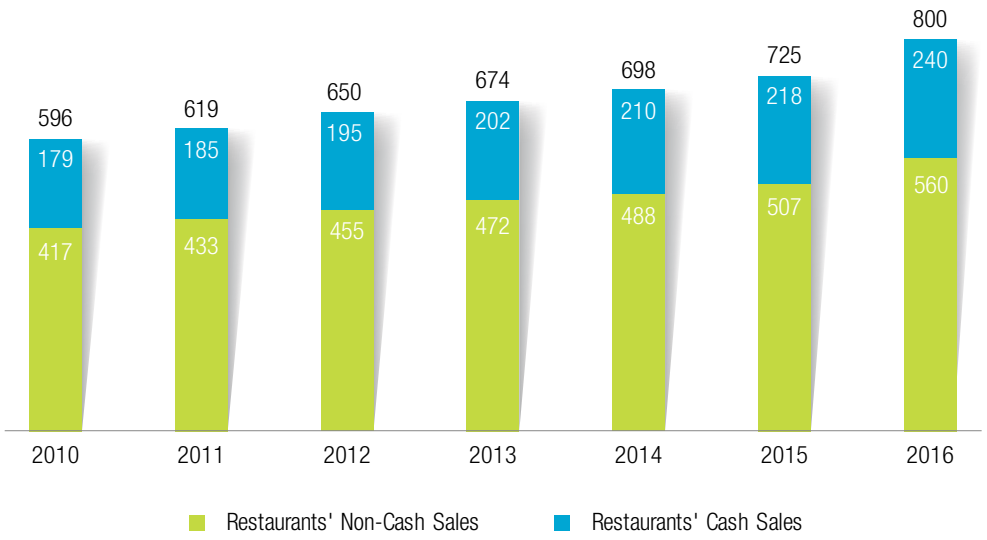
There are many instances of zapping cases now coming to the fore. For instance, in February 2016, a restaurant in Washington State was charged with using a Zapper to hide cash sales and pocket about $395,000[11]. A key driver of zapping fraud is the growing restaurant sales in the US (see Figure 4). Our estimates indicate that Zapping accounts for losses amounting to $3 billion in 2015 in the US. In the EU, it is estimated to be around $2.7 billion.

Third-Party Payroll Processing is Creating Avenues for 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, an owner of a third-party payroll processing firm in the US was sentenced to more than 11 years in prison for embezzling over $17 million from client companies[12]. In the UK, payroll fraud is estimated to cost businesses as much as £12 billion per year[13].

The rising menace of digital tax fraud is proving to be a difficult one to tackle using conventional means. In the following sections, we attempt to quantify the evolution of digital tax fraud in the years leading up to 2020 and suggest measures to curtail it.

Figure 4: Restaurants' Estimated Non-Cash & Cash Sales Split, US, in $ billions



Source: Capgemini Analysis; Study by Federal Reserve Bank of Boston; National Restaurant Association and Restaurant.org forecast; POS Forecast: 2012-2017, Javelin Strategy & Research

Burgeoning Digital Fraud Warrants a Stronger Response

Tax Authorities Need to Drastically Step Up Efforts to Restrain Digital Fraud

To understand the potential impact of digital fraud on tax authorities, now and in the future, we have built a comprehensive forecasting model that assesses the evolution of digital tax fraud in US and EU. This model is based on a combination of relevant data points from the past and proxies (see the research methodology at the end of the paper for details).

As Figure 5 illustrates, we envisioned three different scenarios:

- Scenario 1; in which no specific measures were taken to overcome new types of tax frauds
- Scenario 2; in which incremental solutions were implemented to detect and prevent emerging tax fraud
- Scenario 3; in which a step change and a transformative approach was taken, putting in place comprehensive technological and governance measures

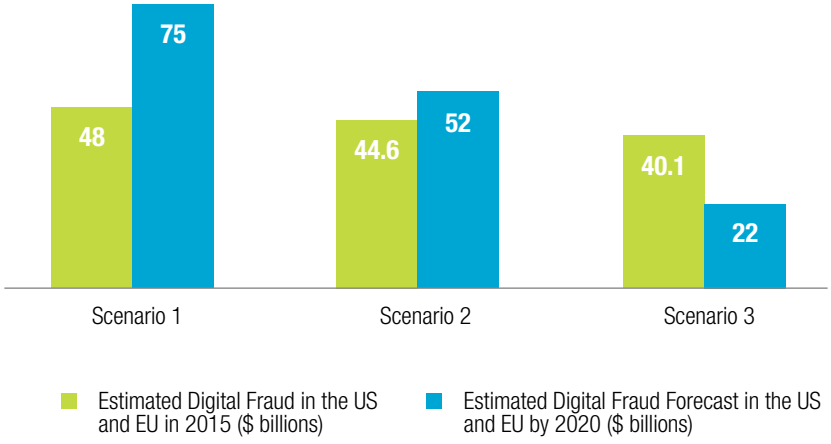
As evidenced in the adjoining table, Scenario 1, in which tax authorities continue to rely on as-is means of fighting digital tax fraud, we estimate that digital tax fraud in the US and EU could rise from $48 billion to $75 billion by 2020, a CAGR of 9.3% .

In scenario 2, in which the tax authorities take incremental measures to check the growth of tax fraud, we estimate that the US and EU digital tax fraud could be constrained to $53 billion, a 3.1% growth over the 2015 estimate. Note that the quantum of tax fraud will still be massive, only its expansion will be subdues to an extent.

However, in scenario 3, we estimate that if tax authorities step up their response and adopt a transformative approach, they would be able to rein in tax fraud to $22 billion by 2020.

Figure 5: The Evolution of Digital Tax Fraud in the US and EU ($ billions)

Scenarios	Details	Estimated Digital Fraud in the US and EU in 2015	Estimated Digital Fraud Forecast in the US and EU by 2020	CAGR
Scenario 1	No measures taken to overcome new types of tax frauds	48	75	9.3%
Scenario 2	Incremental solutions implemented to detect and prevent emerging tax frauds	44.6	52	3.1%
Scenario 3	Step change and a transformative approach that puts in place comprehensive technological and governance measures	40.1	22	-11.3%



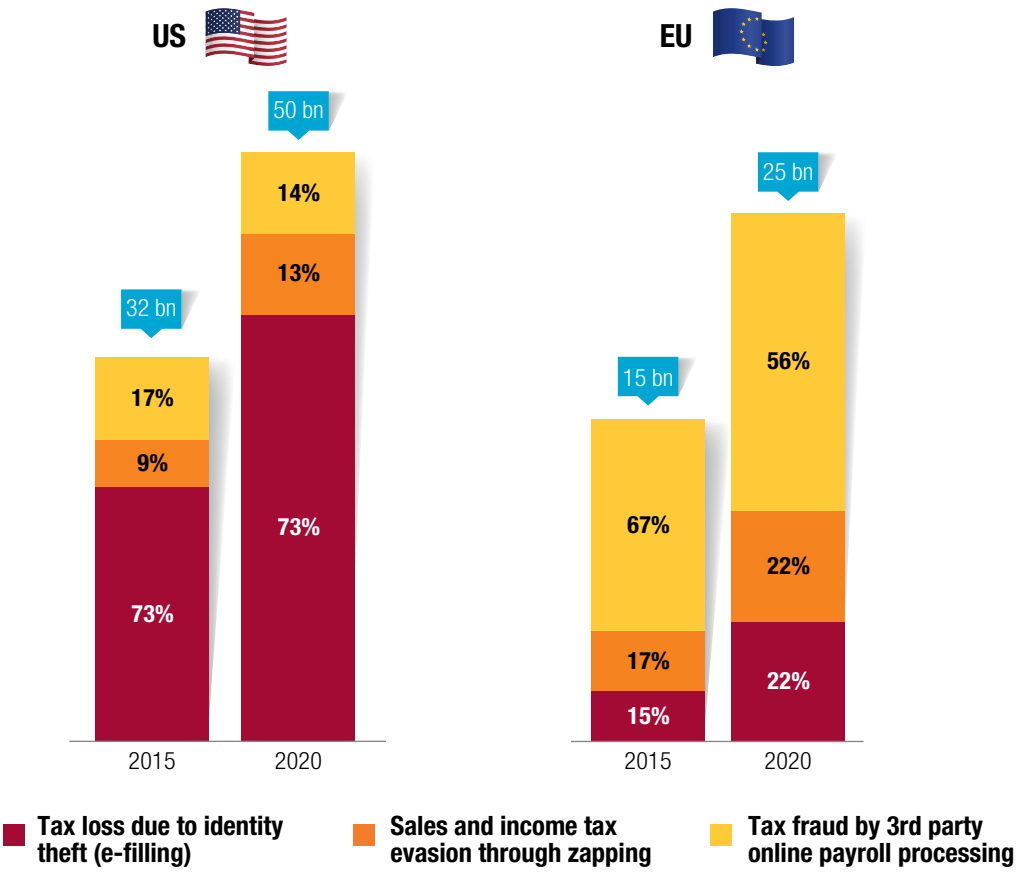
Source: Capgemini Analysis

Efforts to rein in Digital Fraud will vary by region

Our analysis reveals that even as digital tax fraud is on the rise across the US and EU, its drivers differ between the two regions (see Figure 6):

- In the US, identity theft-related tax fraud is by far the biggest contributor to digital tax fraud. A straightforward driver for this is the higher percentage of e-filings as a percentage of overall personal income tax filings in the US, as compared to EU. In many EU countries, the percentages are in the low double-digits. In the US, over 90% returns are e-filed. In the case of Zapping, we forecast tax loss to more than double to reach over $6.5 billion by 2020 from 2015's $3.1 billion.
- In 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: the larger employment base in the SME (Small and Medium Enterprise) sector, higher payroll deductions by the employers, and a greater propensity to outsource payroll processing in the EU compared to the US (55% vs. 40% of firms using third party payroll services[14]).

Figure 6: Breakdown of Forecasted Digital Fraud under 'as is' Scenario 1 (US and EU, 2015-2020), in $ billions

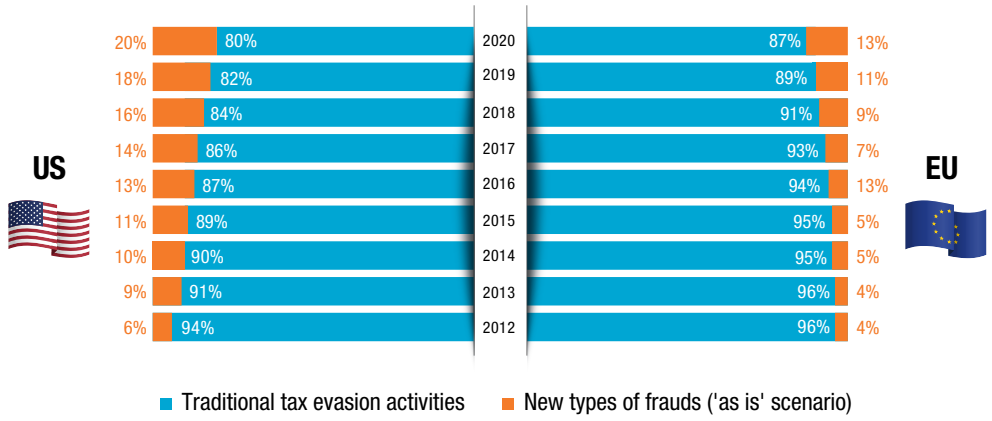


Source: Capgemini Analysis

Growth in Digital Tax Fraud is Driving a Shift in Fraud Mix

Newer types of fraud will grow much more rapidly than the rate at which traditional fraud is declining. In an as-is scenario, where authorities do not make additional efforts to tackle digital fraud, the overall fraud mix will see significant change. We estimate that in the US, by 2020, a fifth of all fraud will be digital in nature. In the EU, digital fraud is expected to account for as much as 13% of all fraud by 2020 (see Figure 7).

Figure 7: Projected Trend of Traditional and New Types of Tax Fraud (US and EU)



Source: Capgemini Analysis

Targeted Interventions Can Significantly Cut Emerging Fraud

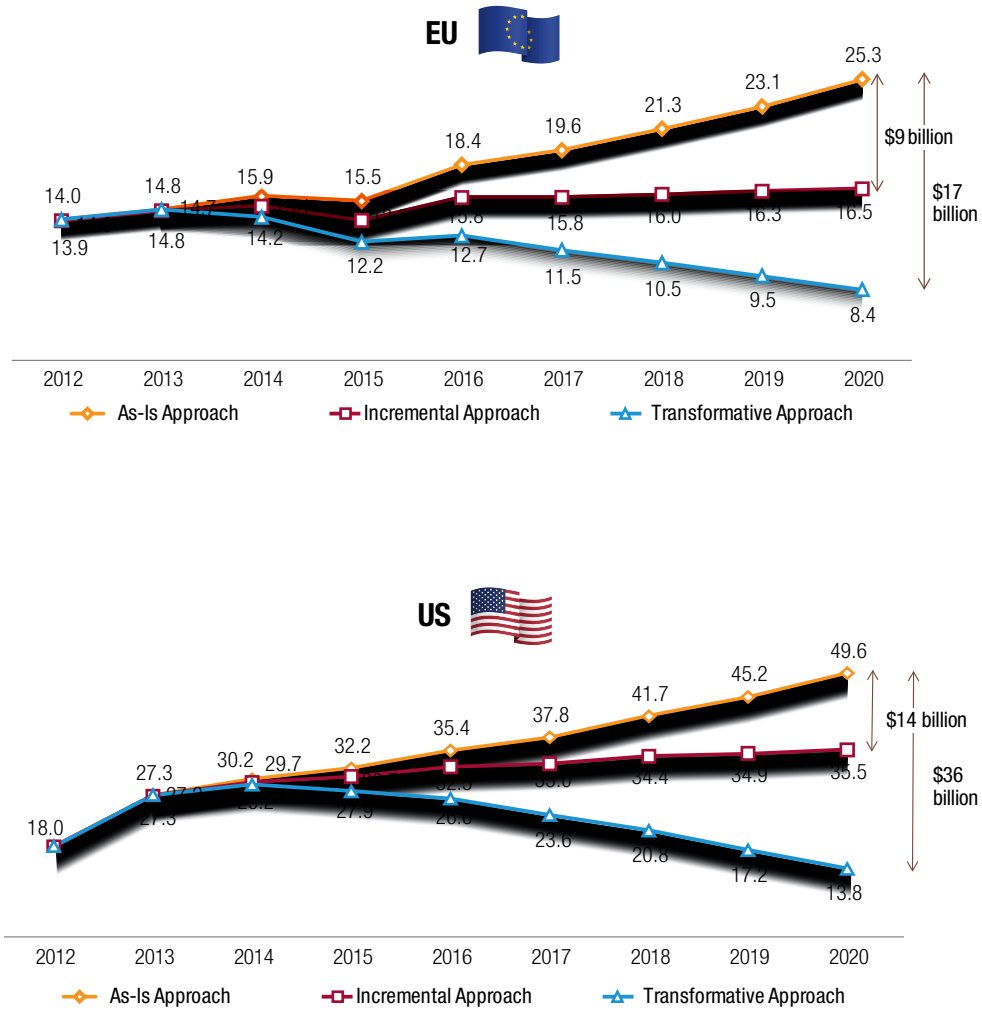
Smart technologies will be key to combating digital fraud. In Australia, authorities are actively monitoring social media to identify tax and welfare frauds. In one instance, authorities caught a couple who were pretending to be two single individuals and claiming welfare funds separately. The two individuals were detected as a result of a Twitter feed announcing they were a couple and were having a baby together[15].

There are two broad approaches tax authorities can take to fight the rise of digital fraud (see Figure 8):

- **The incremental approach:** Here, the authorities can deploy multiple discrete solutions to prevent new types of fraud in the short to medium term. For instance, an OECD report cites several techniques such as e-audit, use of digital forensic tools and even undercover operations that can aid auditors and investigators unearth zapping scams and deter further malpractices[16]. While measures may be effective individually, this approach lacks the synergies of a coordinated response. For instance, in 2012, the US IRS set up as many as 21 departments looking at identity theft[17]. The IRS subsequently realized the limitations of such an approach and set up one centralized unit to look at all identity theft issues[18]. We estimate that by 2020, the incremental approach could save the US and EU tax authorities $14 billion (29%) and $9 billion (35%) respectively in reduced digital tax fraud.

- **The transformative approach:** As explained, incremental solutions can only deliver limited benefits to tax authorities. In a transformative approach, authorities put in place comprehensive technological and governance measures. These initiatives include creating a long-term vision, adopting a clear roadmap and investing in multi-faceted solutions involving people, processes and technology. The potential of such an approach is clear. We estimate that, by 2020, the transformative approach could save the US and EU tax authorities $36 billion (72%) and $17 billion (67%) respectively in mitigated fraud. An example of a transformative approach is the "Reinventing the Australian Taxation Office" (ATO) initiative[19]. This comprehensive program aims to make the ATO a smart, service-oriented organization by undertaking a thorough transformation delivered via six strategic programs that cover technological, cultural and organizational imperatives:
  - Smarter data
  - Optimized workforce capability and culture
  - Tailored engagement and support
  - Governance, design and evaluation
  - Contemporary digital services
  - Working with partners in the tax and super systems

Figure 8: Impact of Digital Solutions in Curtailing Digital Fraud (US and EU, $ billion)



Source: Capgemini Analysis

Analytics: a Potent Weapon in the War against Digital Tax Fraud

Digital tax fraud does not stand still – it is in a constant state of flux. As new digital technologies and platforms continue to emerge, so will different types of tax fraud. This calls for innovative ways to tackle emerging exposures and requires that tax authorities become digital tax authorities. The digital tax agency of tomorrow will leverage new data sources as well as sophisticated analytics to combat new digital frauds and to nudge people to be more compliant in real-time. In this section, we present a suggested roadmap for tax authorities for implementing solutions to counter new fraud developments.

Assess the Extent of Digital Fraud. Tax authorities need to identify emerging digital tax fraud and assess their spread and financial impact, using pilot projects to analyze incidence. The Canada Revenue Agency ran a three-year pilot 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[20]. 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. Regular audits can reveal loopholes and missing capabilities. For instance, the IRS uses a series of filters to flag potentially fraudulent returns, but found that the majority of the tax returns that were initially flagged were eventually deemed legitimate, revealing that the accuracy of the screening filters was the issue. Missing capabilities can then be prioritized using a heat-map that reflects the potential amount of tax fraud averted as a result of adding a capability. The optimum capabilities are then prioritized. Many tax authorities are realizing the importance of cybersecurity safeguards and related capabilities. Following an unprecedented four-fold jump in identity-theft cases between 2011-14, the IRS decided to create a cyber investigative team to focus on cases of tax frauds involving cyber crime[21].

Define Vision and Target Operating Model. The IRS, for example, defined a vision based on implementing a Real-Time Tax System. The system would allow matching of data on tax returns with data in IRS's records at the time the tax return was submitted for filing. It is important that technology solutions are delivered in tandem with any changes also necessary to the operating model and organizational structure.

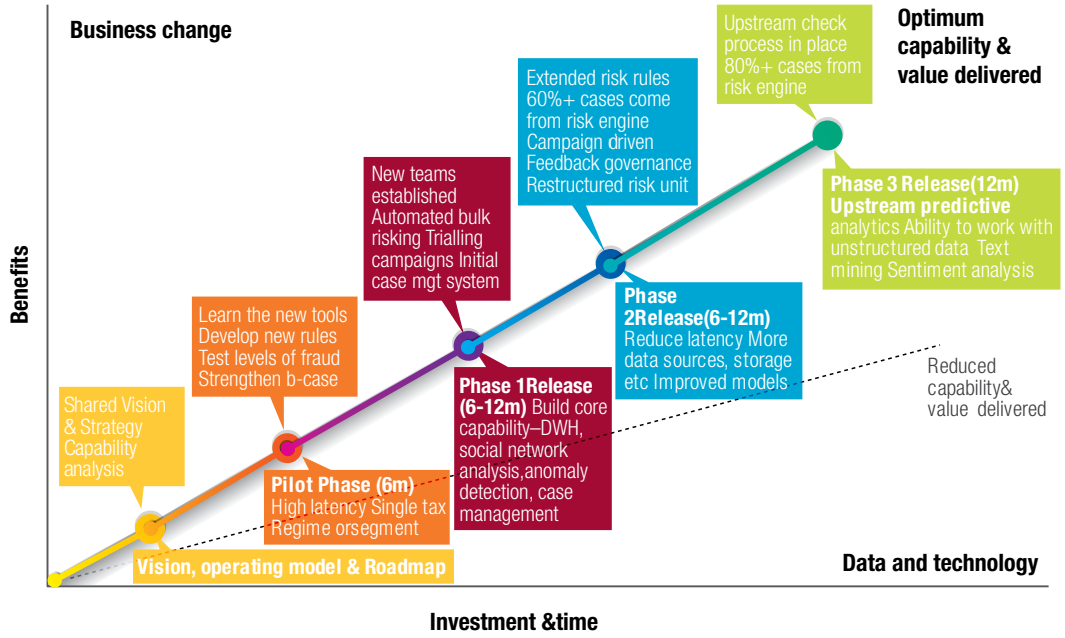
Develop an Integrated Solution Comprising Policy, Processes, People and Technology. An integrated approach is necessary as leaving out any essential component would render the entire transformation ineffective. Policies including the legislation and guidelines need to be drafted to discourage fraudulent behavior. 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[22]. Employees need to be engaged with new ways of tackling fraud, and taxpayers and welfare recipients need to be educated on the risks of identity theft. Tax authorities must constantly refresh their understanding of new technological platforms that can be used to enhance the citizen experience, while combating fraud. Tax authorities must also raise awareness among the general public regarding potential sources of tax fraud and their risks. For instance, during the peak of tax filing season every year, IRS publishes a list of top scams and frauds, so that the taxpayers remain vigilant about them[23].

Adopt an Agile Implementation Approach. Traditional approaches to addressing tax fraud have been packaged in long, elaborate programs with gestation periods spanning months and, in some cases, years. However, the pace of newer digital tax frauds shows that this approach is no longer appropriate and falls well short of achieving rapid results. Running pilot projects to test aspects of the potential solution will help prioritize the rollout of new capabilities and control costs. 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. A range of technologies, such as machine learning, network analytics, predictive modeling, text analytics, social media monitoring, anomaly detection and their cybersecurity applications, could help achieve this.

Getting Started and Key Challenges

Each tax administration is at a different starting point, and therefore, will require a roadmap tailored to their individual situation and priorities. An indicative roadmap with timelines is shown in Figure 9.

Figure 9: A Generic Roadmap for Tax Authorities to Build Analytics Capabilities



Source: Capgemini Analysis

It is important to bear in mind that combating digital fraud is not principally a technology challenge. The real challenges lie in securing the right data and permissions; putting in place the necessary governance and master data management to ensure quality data; and above all understanding and successfully implementing changes to processes, procedures and people's roles. In particular, implementing an analytically-driven approach to risk has major cultural implications. Highly-trained compliance investigators will be required to take up cases that have been selected by the algorithms rather than using their own judgment and intuition. The success of the implementation will depend on factors such as current capability, availability of and ability to use data, the nature of the priority compliance risks and political imperatives.

Conclusion

Revenue loss through digital tax fraud is a significant burden for countries that are currently struggling to rein in their fiscal deficit. Digital tools are critical weapons in their armory as they fight fraud. Digitization, however, is also giving rise to new exposures. While traditional fraud is on the decline, fraudsters are exploiting the loopholes and possibilities of a more connected world. Unless government authorities stay one step ahead on the digital curve, the fraudsters could win the digital tax war.

Research Methodology:

Forecasting fraud, particularly that enabled by new technologies in an age of rapid change, is not a straightforward task. Capgemini built a forecasting model to estimate the impact of digital fraud in the US and the EU from 2016 through to 2020, by analyzing the three fast-growing frauds – identity theft, zapping, and third-party online payroll processing fraud. Given that the fraud categories we looked at are quite recent, there is not significant historical data available. We estimated the growth of each fraud class through a combination of data points and proxies for which we had historical figures and were considered relevant to the task at hand. For instance:

For Identity Theft related Tax Fraud: Parameters to estimate this included: the overall employed population, the projections of the population, the number of returns where ID theft was an issue, the value of the fraud itself, the number of e-filed returns that experienced ID theft, the number of e-file returns, the total value of ID theft.

For Zapping: The most common source of Zapping is restaurants. In order to forecast the value of Zapping-related fraud, we analyzed data related to: restaurant sales, the percentage of cash transactions at restaurants, third-party surveys on average use of zappers in the restaurant community, average sales and corporate taxes that restaurants pay, average financial performance of restaurants.

For Payroll Processing Fraud: We looked at a variety of employment data to estimate the extent of this fraud. This included: annual payroll data, growth in payroll from the late 90s, total social security and Medicare (in the US), income tax data, surveys on firms using third party payroll services, contribution of categories of firms such as SME to employment, number of employees in such SMEs and other employment data.

Capgemini's Solution to Combat Tax & Welfare Evasion and Fraud in the Digital Age

Capgemini has extensive experience in helping government agencies to combat tax evasion and welfare fraud, and to protect tax yield through detection and prevention.

Our Fraud & Criminal Behavior detection solutions leverage our considerable experience in Big Data and advanced analytics to address these issues. We combine our extensive expertise in several domains (including crime & cybersecurity, tax & welfare and financial services) as well as bring a wide range of leading prevention techniques.

Capgemini's tax evasion and welfare fraud solution takes a step-by-step approach, using the SAS® Fraud Framework and customer intelligence software, to diagnose fraud, assess threats, analyze customer behavior and optimize the fraud management process.

We use Big Data technologies to analyze all the disparate data for near real-time fraud detection and prevention, and provide leading data analysis and pattern recognition to rapidly assess threats to an organization.

Behind these capabilities, we have defined the people, process and organization changes required, as well as the business services, information services, technical architecture and components needed to deliver the major priorities identified by tax and welfare agencies, such as detecting internal fraud and collusion, and securing online channels.

We have worked with tax and welfare agencies from around the world including Europe and Asia, where we have put in place fraud protection systems and processes that sit within a defined anti-fraud framework.

Examples include:

- Design, build and deployment of a strategic risking tool that cross-matches one billion internal and third party data items to uncover hidden relationships across organizations customers and their associated data links;
- Implemented a fraud solution based on the SAS® Fraud framework to combat VAT carrousel fraud, involving technology & data, advanced analytics and additional business change initiatives to cement the adoption of the new fraud model within the client organization. The solution resulted in a ROI of a factor 20 and prevented millions of Euros of wrongful payouts each year;
- Implemented an end-to-end business intelligence, data warehousing, and reporting solution from scratch, including installation of hardware, software, solution definition enabling the client to close the gap between revenue owed and collected, and to detect erroneous patterns of financial reporting.

In addition, our Assurance Scoring solution provides better customer service and fraud protection; Our predictive analytics solution improves assurance, so that low-risk transactions or customer applications can be confidently identified for automatic processing and therefore staff can be redeployed to focus on high risk investigations of potential problems.

References

1 Fortune, “Here’s How Much Tax Cheats Cost the U.S. Government a Year”, April 2016

2 The Guardian, “UK tax fraud costs government £16bn a year, audit report says”, December 2015

3 European Commission, “VAT Gap: Nearly €160 billion lost in uncollected revenues in the EU in 2014”, September 2016

4 SAS.com, “How hybrid fraud detection cut losses by 98% in Belgium.”, Accessed October 2016

5 Australian Taxation Office, “Reinventing the ATO”, Accessed October 2016

6 CNBC, “Tax-refund fraud to hit $21 billion, and there’s little the IRS can do”, February 2015

7 Kluwer Law Online, “Turbo Liquidation of a Company : An Open Invitation to Commit Fraud?”, 2016

8 BBC, “Identity fraud up by 57% as thieves ‘hunt’ on social media”, July 2016

9 Internal Revenue Service, “Consumers Warned of New Surge in IRS E-mail Schemes during 2016 Tax Season; Tax Industry Also Targeted”, February 2016

10 Federal Trade Commission, “FTC Releases Annual Summary of Consumer Complaints”, March 2016

11 The Seattle Times, “Bellevue restaurant accused of tax cheating”, February 2016

12 FBI, “Operator of Third-Party Payroll Company Sentenced to More Than 11 Years in Prison for Embezzling $17 Million from Client Companies”, December 2015

13 CIPD, “Payroll fraud costs UK firms £12bn per year”, May 2016

14 National Small Business Association, “2013, Small Business Technology Survey”, 2013

15 The Daily Telegraph, “Welfare fraud: Government hunting down cheats found through their social media posts”, February 2016

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

17 IRS, “Annual Report to Congress”, 2012

18 IRS, “Annual Report to Congress”, 2015

19 Australian Taxation Office, “Reinventing the ATO”, Accessed October 2016

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

21 The Hill, “IRS sets up cyber investigative team amid surge in tax fraud”, May 2015

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

23 IRS, “IRS Wraps Up the “Dirty Dozen” List of Tax Scams for 2016”, February 2016

About the Authors

Philippe Kerael
Vice President, Insights and Data, Risk & Compliance & Fraud Analytics Head
philippe.kerael@capgemini.com

Philippe is the Global head of fraud, risk and compliance at Capgemini. He is based in France.

Jerome Buvat
Head, Digital Transformation Institute
jerome.buvat@capgemini.com
@jeromebuvat

Jerome is head of Capgemini's Digital Transformation Institute. He works closely with industry leaders and academics to help organizations understand the nature and impact of digital disruptions.

Subrahmanyam KVJ
Senior Manager, Digital Transformation Institute
subrahmanyam.kvj@capgemini.com
@Sub8u

Subrahmanyam is a senior manager at the Digital Transformation Institute. He loves exploring the impact of technology on business and consumer behavior across industries in a world being eaten by software.

Ashwin Gopakumar
Manager
ashwin.gopakumar@capgemini.com

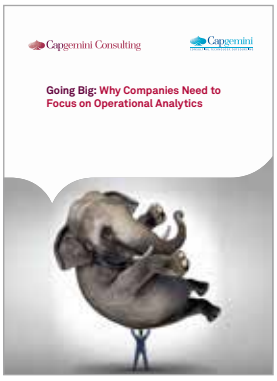
Ashwin is a manager at Capgemini Consulting India. He is passionate about understanding the latest trends in digital technology and loves to help clients on their digital journey.

Digital Transformation Institute
dti.in@capgemini.com
The Digital Transformation Institute is Capgemini's research center on all things digital.

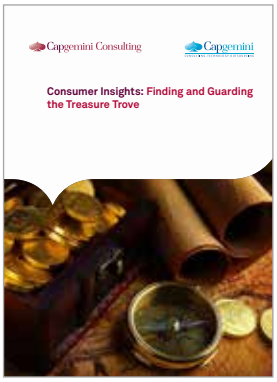
The authors would like to thank Amol Khadikar and Aritra Ghosh from the Digital Transformation Institute for their contribution to this research paper.

Discover more about our recent research on digital transformation

Fixing the Insurance Industry: How Big Data can Transform Customer Satisfaction



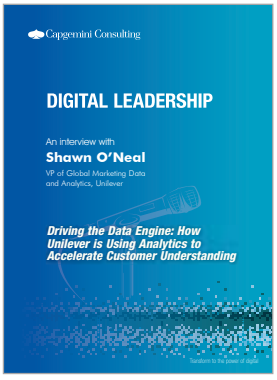
Going Big: Why Companies Need to Focus on Operational Analytics



Consumer Insights: Finding and Guarding the Treasure Trove

Privacy Please: Why Retailers Need to Rethink Personalization

Cracking the Data Conundrum: How Successful Companies Make Big Data Operational



Driving the Data Engine: How Unilever is Using Analytics to Accelerate Customer Understanding

Big Data BlackOut: Are Utilities Powering Up Their Data Analytics?

Organizing for Digital: Why Digital Dexterity Matters

Stewarding Data: Why Financial Services Firms Need a Chief Data Officer

For more information, please contact:

Global:

Philippe Kerael
philippe.kerael@capgemini.com

Daan Landkroon
daan.landkroon@capgemini.com

Belgium, Netherlands and Luxembourg
Liesbeth Bout
Liesbeth.bout@capgemini.com

China
Pingjie Gao
pingjie.gao@service.capgemini.com

Germany, Austria and Switzerland
Ingo Finck
Ingo.finck@capgemini.com

United Kingdom
Nigel Lewis
Nigel.b.lewis@capgemini.com

India
Manik Seth
Manik.seth@capgemini.com

North America
Ashley Skyrme
Ashley.skyrme@capgemini.com

Norway
Erlend Selmer
Erlend.selmer@capgemini.com

Spain
Jose Ignacio Reboredo Canosa
Ignacio.reboredo@capgemini.com

Sweden and Finland
Mats Hovmoller
Mats.hovmoller@capgemini.com

France
Laurence Chrétien
Laurence.chretien@capgemini.com

Charlotte Pierron-Perlès
Charlotte.pierron-perles@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, the global team of over 3,000 talented individuals work with leading companies and governments to master Digital Transformation, drawing on their understanding of the digital economy and leadership in business transformation and organizational change.

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

Rightshore® is a trademark belonging to Capgemini

About Capgemini and the Collaborative Business Experience

With more than 180,000 people in over 40 countries, Capgemini is a global leader in consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, 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.capgemini.com.