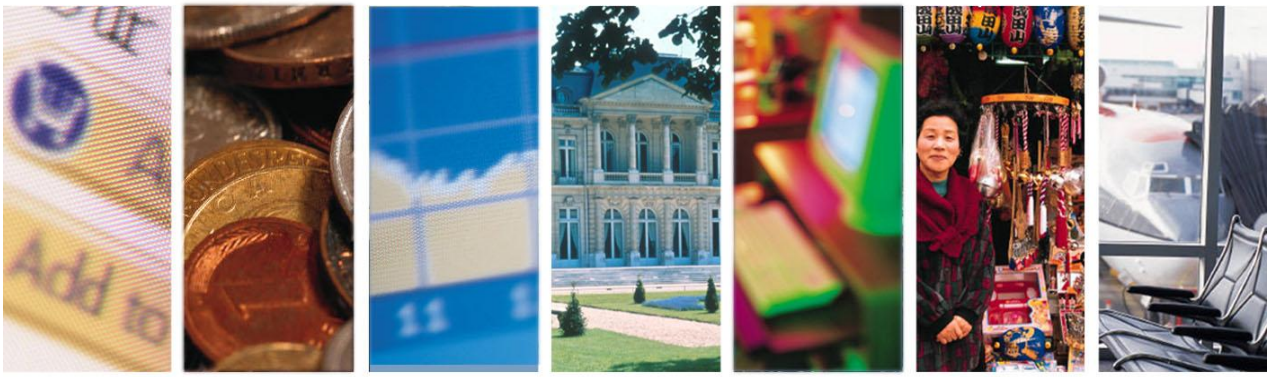
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT



REPORT ON IDENTITY FRAUD: TAX EVASION AND MONEY LAUNDERING VULNERABILITIES

2006

CENTRE FOR TAX POLICY AND ADMINISTRATION

EXECUTIVE SUMMARY

Identity related crime is a serious and increasing risk in many countries although its impact is variable. Some countries estimate that identity fraud overall costs their economies billions of dollars and is becoming more organised and more sophisticated. There are few estimates for the costs of identity fraud in terms of lost tax revenue. This report provides the results of a survey of the 19 countries which are members of the Sub-Group on Tax Crimes and Money Laundering to assess the tax crime and money laundering vulnerabilities associated with identity fraud.

The report compiles the common methods of identity fraud encountered the sectors at risk and the few attempts so far to quantify those risks. It sets out the detection strategies that countries have adopted and importantly provides a listing of red flag indicators which countries can use in training tax auditors. The report Gives examples of information resources and describes the investigation approaches adopted by a number of countries. The report gives illustrative case studies to aid comprehension and give practical guidance to tax authorities that are seeking to implement or refine their strategies to effectively address the risks of identity fraud.

TABLE OF CONTENTS

REPORT ON IDENTITY FRAUD: TAX EVASION AND MONEY LAUNDERING VULNERABILITIES

I. Background:

1. Identity related crime is regarded by many countries as a serious and increasing risk to governments and the wider community. Some countries suggest that identity fraud is costing their economy billions of dollars in terms of lost tax revenue, overpayment of social security claims and losses incurred by consumers, banks, credit card firms, retailers and other businesses. Identity fraud manifests itself in many different forms, such as credit card fraud, stealing money from individuals' bank accounts through telemarketing schemes, income tax refund fraud and social security fraud. There is evidence to suggest that identity crime is becoming more organised, rather than opportunistic, particularly with regards to identity theft. The increasing use of sophisticated electronic means and the associated speed of processing claims etc. provide significant challenges for tax authorities to quickly implement effective controls. The level of sophistication also increases the difficulty of detection of this type of crime and the apprehension of offenders.

2. Taking into account the significant risks outlined above, delegates of the Working Party No. 8 Sub-Group on Tax Crimes and Money Laundering (TCML) agreed in March 2006 to examine the tax evasion and money laundering vulnerabilities associated with identity fraud. To facilitate this examination, the Secretariat distributed questionnaires to Sub-Group delegates and it was agreed that the information contained in the responses would be used as the basis for preparing a comprehensive report on the topic.

3. This report contains information on the tax evasion and money laundering vulnerabilities associated with identity fraud[1]. The information contained in this report was provided by 19[2] countries represented on the Sub-Group in response to the questionnaire that was sent to delegates in July 2006. Apart from providing a useful overview of the key tax evasion and money laundering issues and risks associated with identity fraud, the report is also intended to provide practical guidance to tax authorities that are seeking to implement strategies to effectively address these risks. The report is also intended to assist tax authorities in refining their existing strategies.

4. The report specifically addresses:

a. Definitions and examples of identity fraud;

b. Quantifying the risks associated with identity fraud;

---

1 This report does not cover "concealing identity" issues (e.g. methods to conceal beneficial ownership).

2 Argentina, Australia, Austria, Canada, Czech Republic, Denmark, France, Germany, Ireland, Japan, Mexico, Norway, Portugal, Slovak Republic, Spain, Sweden, Turkey, United Kingdom and the United States.

c. How countries detect suspected cases of tax evasion and money laundering involving identity fraud;

d. "Red Flag Indicators" used to detect identity fraud;

e. How countries investigate cases of suspected tax evasion and money laundering involving identity fraud;

f. Effective measures undertaken by tax and other government agencies to increase compliance and deter non-compliance in these areas; and

g. Results of activities designed to detect and address non-compliance, and to promote compliance.

Definitions and examples of identity fraud

What is identity fraud?

5. Identity fraud and identity theft are often used to describe any situation in which personal details are misappropriated for gain. Examples of identity fraud include using a false identity or someone else's identity details (e.g. name, address, previous address, date of birth etc.) for commercial, economic or monetary gain; or obtaining goods or information; or obtaining access to facilities or services (such as opening a bank account, applying for a benefit or obtaining a loan/credit card). The following definitions have been developed by the United Kingdom's Home Office Identity Fraud Steering Committee[3] to clarify these terms.

6. **Identity crime** is a generic term for Identity Theft, creating a False Identity or committing Identity Fraud.

7. False identity is:

a. a fictitious (i.e. invented) identity; or

b. an existing (i.e. genuine) identity that has been altered to create a fictitious identity.

8. **Identity theft** occurs when sufficient information about an identity is obtained to facilitate Identity Fraud, irrespective of whether, in the case of an individual, the victim is alive or dead.

9. **Identity fraud** occurs when a False Identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Fraud.

---

[3] The Home Office Identity Fraud Steering Committee comprises:

APACS - the UK payments association
Association of Chief Police Officers
British Bankers' Association
CIFAS, the UK's Fraud Prevention Service
Department for Constitutional Affairs
Department of Work and Pensions/Jobcentre Plus
Driver and Vehicle Licensing Agency
Finance & Leasing Association
Financial Services Authority
HM Revenue & Customs
Home Office
Identity and Passport Service
Telecommunications UK Fraud Forum

10. These definitions are not legal definitions and are not tied to specific criminal offences, and they apply to both individual and corporate Identity Crime.

II. Survey Findings and Observations

Common methods and schemes used to commit tax evasion and money laundering involving identity fraud.

11. Several methods and schemes involving false identities and identity theft to facilitate tax evasion and money laundering have been detected by the tax authorities that participated in the survey. The most commonly detected methods and schemes reported include:

- Creation or takeover of a person's identity for the purpose of lodging false claims for refunds and rebates (e.g. filing of false individual income tax returns, using false information and documents, to obtain income tax refunds and GST credits);
- Use of false and stolen identities to set up businesses to commit income tax and GST/VAT fraud;
- Creation of an identity on the basis of a stolen/fraudulently used passport or other major source of identification, which is used to obtain a national identification number, which in turn is used for social welfare claims, for tax or business registration, opening bank accounts, printing invoices, etc;
- Theft of correspondence from the tax authority and the use of those details to obtain employment or to falsely claim repayments on medical expenses, etc., having changed the contact details;
- Creation of shell companies that do not conduct real operations, but only simulate transactions to generate a refund or credit against VAT;
- Carousel fraud, in which a shell company manager uses a bogus identity or stolen identity.
- Creation of shell companies that do not conduct real operations, but put money into circulation through bad cheques taken from banks with false identity and documents;
- Fraudulent use of documentation of suppliers with which no business was conducted, with the purpose of reducing the applicable income tax rate or to generate fictitious losses;
- Deposit of large sums of cash that are subsequently transferred to other accounts, in several countries, so that the money is transferred to legal businesses (in this case the person with the false or stolen identity might be the owner or authorised on the first or second bank account);
- Use of the identities of immigrants who have returned to their home countries by relatives or other persons to continue receiving benefit payments;
- Hijacking of client's identity by agent who uses it to commit fraud;
- Filing of claim by agent for person who does not exist – "bogus claim";
- Nomination of a bank account not in the name of the claimant;
- Taking advantage of vulnerable individuals to secure private password details, gain illegal access to systems and manipulate to fraudulent personal advantage;
- Thieves attempting to gain access to identifying information maintained at major depositories of personal data (e.g. government agencies, banks). This access can take the form of computer intrusion (hacking), compromise of employees with authorized access to the data (corruption), or deception;
- Use of computers and other means of deception to obtain identifying information directly from the individual (e.g. "phishing", "spyware" and "skimming"); and

- Use of the Internet to obtain information of companies making sales on the Internet, for the purpose of transferring money from those companies' accounts to personal accounts opened by using a false identity.

Case studies: Methods and schemes used to commit tax evasion and money laundering using identity fraud:

Canada: False and stolen identities have been used to set up businesses to commit GST fraud and to file false income tax returns in Canada. The filing of false individual income tax returns, using false information and documents, to obtain income tax refunds and GST credits has also been a problem. There have been cases where tax return preparers have inflated the refunds claimed on their clients' returns and kept the difference or used old client information to file false returns and appropriated the refunds.

France: Identity fraud is also beginning to crop up in the advertising agency sector. This type of scam involves identity and corporate identity theft to extort money from firms to which the bogus advertising agency has "sold" advertising space. Sometimes, the advertising agency's clients are in on the scheme and use this stratagem to lower their tax base. This scheme is sometimes connected with money laundering.

Mexico: Individuals create "fake" official identifications; for example, using data from third parties and placing the delinquent photo in an Official ID, with the purpose of constituting a business, opening bank accounts, creating contracts and printing invoices. Criminals undertake operations using fake IDs and do not report any income. They disappear shortly after without having paid any taxes and, in the worst cases, launder money generated from illicit sources. When the tax authority detects the omission in the payment of taxes, the investigation begins with the original owner of the ID who does not recognize the operations and a long process begins of trying to identify the real offender. This situation seriously affects the efficiency and costs of the Ministry of Finance and Public Credit.

United States: Large-scale breaches of data repositories – Thieves attempt to gain access to identifying information maintained at major depositories of personal data. This access can take the form of computer intrusion (hacking), compromise of employees with authorized access to the data (corruption), or deception. Some of the major depositories that are vulnerable to large-scale breaches are government agencies, bank records, credit card systems, credit report companies, and Internet companies that require identifying information to use their services such as on-line gambling. For example, employees at large businesses have a variety of records to choose from to steal ID information, including job applications, personnel records, health and benefit records, and payroll records.

Large-scale breaches of data from individuals – Thieves using computers and other means of deception to obtain identifying information directly from the individual. Common techniques that fall within this category include (1) "Phishing" - Criminals will portray themselves as legitimate organizations that would normally need this information, such as banks, credit card companies, and government entities. For example, criminals have portrayed themselves as being IRS employees to get ID information. Taxpayers are sent e-mails purportedly from an IRS website falsely informing them that there is a problem with their tax returns and requesting ID information in order to resolve the problem. Another example focuses on foreign citizens that have assets in the U.S. Fictitious IRS Form W-8 BEN will be sent to foreign citizens to trick them into disclosing their personal and financial data; (2) "Spyware" and other computer software programs designed to gain access to Internet users' computers and data without the user's permission; (3) * "Skimming" – An inexpensive device that resembles a credit/debit card processor that when a card is passed through it records the magnetically encoded identifying data recorded on the card. Another form of skimmer is being placed on automatic teller machines (ATMs) to obtain the data associated with the ATM card when it is inserted in the device; and (4) Unscrupulous tax return preparers and individuals will steal social security numbers from their clients or acquaintances.

Which sectors and occupational groups are potentially affected by identity fraud?

12. Identity fraud potentially affects all sectors and occupational groups. However, the countries surveyed report that the following sectors are particularly vulnerable to the use of false identities and identity theft:

- Services sector (e.g. catering, cleaning, security);
- Any sector that would be in a credit position for VAT/GST purposes (e.g. exporters);
- Tax return preparers, accountants, lawyers and other gatekeepers (or intermediaries);
- Construction industry;
- Unlicensed foreign exchange houses;
- Real estate sector (including purchase and sale of real estate);
- Sale of motor vehicles, yachts, second hand vehicles and industrial machinery;
- Scrap metals industry;
- Casinos and other entertainment venues (e.g. bars, nightclubs);
- Professionals and individuals connected with sports and entertainment;
- Art dealers and precious stones;
- Activities related to the exploitation of land (cork, wood, etc);
- Temporary work companies;
- Hardware wholesaler sector;
- Any large payroll database is an attractive prospect to an organised ID hijacker (e.g. supermarkets);
- Rogue agents in the immigration services sector;
- Financial institutions;
- Retailers (including Internet retailers);
- Telephony and computer components sectors; and
- Government entitlement programmes.

Case study: United Kingdom research into areas of vulnerability

The United Kingdom's Home Office Identity Fraud Steering Committee has commissioned research into areas of vulnerability, for example, use of identity data belonging to deceased persons to commit identity crimes. For further details see www.identity-theft.gov.uk.

Research has been undertaken by various organisations and groups such as CIFAS (the UK fraud advisory service) to determine which occupational groups, industries/sectors and individuals are particularly vulnerable to identity crime. For further details see www.cifas.org.uk.

Quantifying the risks associated with identity fraud

13. Most of the countries surveyed have not attempted to quantify the economic cost and/or the level of tax evasion and money laundering associated with identity fraud. However, in the countries that have made such estimations, the amounts are significant.

Examples of economic cost and level of tax evasion and money laundering associated with identity fraud:

The estimated cost of identity fraud in **Australia** is between AUD$1 - 4 billion annually.

In **Canada**, it is estimated that consumers, banks, credit card firms, stores and other businesses lost CAN$2.5 billion to perpetrators of identity theft in 2002.

In **Ireland**, an evaluation in 2000 by the Department of Social & Family Affairs estimated the loss in social security claims to be between €25 million and €50 million per annum.

In **Portugal,** although the level of fiscal fraud in this area is not quantified, it is estimated that it runs into many millions of euros.

In the **United Kingdom**, the Home Office Identity Fraud Steering Committee estimates that identity fraud costs the UK economy £1.7 billion. The latest HM Revenue and Customs (HMRC) estimates for 2005-06 show that attempts to defraud the tax credits system totalled £540 million; of this, HMRC was able to detect and prevent attempts worth £409 million, the vast majority before they were paid out.

In the **United States**, private sector research revealed that approximately 9.3 million adults had been victims of identity fraud in 2003, and that total losses (individual and corporate) from identity fraud exceeded US$52 billion. The research also found that approximately 8.9 million adults had been victims of identity fraud in 2004, and that total losses exceeded US$56 billion. The number of Suspicious Activity Reports (SARs) filed by financial institutions in the United States where identity fraud has been suspected has increased over the last three years. The numbers of SARs filed are 4,112, 17,011, and 23,791 for the years 2003, 2004 and 2005 respectively.

How countries detect suspected cases of tax evasion and money laundering involving identity fraud

Detection strategies and techniques

14. Most of the countries surveyed use a combination of intelligence gathering, risk analysis, risk profiling and data matching to detect cases of tax fraud and/or money laundering using identity theft and

identity fraud. Several countries report that data matching and other information sharing activities between tax authorities and other government agencies are carried out to detect and investigate suspected cases of tax evasion and/or money laundering involving identity fraud.

Case studies: Detection strategies and techniques

Canada: Specialized teams have been established within the Canadian tax authority that verify the integrity of registration data and risk assess new GST registrations against risk criteria such as those who do not appear to have the income to start a business or appear too young to start a business. Other detection strategies include:

- Using specialized high-risk teams that proactively search for potential GST fraud and look for relationships between accounts to identify fictitious entities using internal and external databases.
- Carrying out computerized validity checks for processing credit returns and identifying duplicate returns.
- Profiling of known cases to identify the characteristics of such schemes.
- Establishing a cross-functional working group to study the increase in fraudulent income tax returns and make recommendations to improve identity procedures, systems and practices to curtail this type of fraud.

France: Chief among the national methods used is the power to require disclosure, a procedure that allows an official of the French tax authorities to obtain information from a third party. In this particular case, it enables an official to request an identity check with the National Identity Register, which is under the authority of another administration. National means can also be used in tandem with international administrative co-operation, which is really effective in this area. One example is the European EUROCANET Database which lists the largest telephony and computer component operators. Using this base, member states can run cross-checks placing the operators in question under constant surveillance.

Sweden: The transparency in the Swedish system has prevented identity fraud being used to commit large-scale tax fraud. Every Swedish citizen can check what is registered in different registers. If a person tries to steal an identity at one end of this system, it will always generate a question or a message to the "real person" from another part of the system that something is wrong or must be changed.

United Kingdom:

- Developed random enquiry programmes designed primarily to detect internal fraud but will highlight other issues.
- Developed HMRC's risk assessment process to identify in advance those cases which are likely to be fraudulent, so as to stop them going into payment.
- Embedded compliance specialists in contact centres, thereby providing additional support and specialist knowledge.
- Increased pre-payment checks into claims where fraud or non-compliance is suspected.
- Strengthened co-operation by working closely with other Government Departments and the private sector – for example referrals received under the Proceeds of Crime Act (POCA).
- Use of Suspicious Activity Reports (SARs) under POCA.
- General Risk analysis: Profiling in HMRC data of information from customer self assessment returns and other third party information.
- Directed case selection based upon knowledge of risk of specific industries, for example Construction Industry.

United States:

- The IRS Identity Theft Program Office-Identity Theft Enterprise Strategy: This strategy represents a comprehensive approach to combating identity theft by focusing on outreach, prevention and victim assistance. The outreach component seeks to alert and inform tax professionals, taxpayers, and other interested parties of the threat identity theft poses to tax administration. The prevention component's objective is to proactively address identity theft within the context of tax administration. An example of these activities is the IRS's efforts to identify and deter "phishing" schemes before taxpayers can be victimized. The third prong of the strategy is victim assistance, the important task of mitigating and correcting the harm suffered by taxpayers that are victims of identity theft.

Case studies: Detection strategies and techniques

United States: **continued**

- The IRS Criminal Investigations' Questionable Refund Program (QRP) and Return Preparer Program (RPP) are focused on identifying and stopping fraudulent tax refund claims schemes. These schemes often involve hundreds of returns with refunds totalling hundreds of thousands or even millions of dollars of revenue at stake. Investigating and prosecuting those responsible for these ambitious schemes ranks among the programs' highest priorities. Though identity theft is not a component of all fraudulent refund schemes, the rise of identity theft has helped fuel an increase in fraudulent refund schemes and other tax frauds, specifically employment tax fraud.

15. Most countries report that the strategies and techniques used by their tax authorities to detect tax evasion and money laundering involving identity fraud have been successful in terms of:

- Improving identification of suitable cases to audit;
- Preventing revenue loss through proactive data mining;
- Enabling the prosecution of cases that otherwise may have never been detected; and
- Providing the quickest opportunity to review returns that potentially use a stolen identity before the refunds are issued and thereby likely irretrievable.

What "red flag indicators" are used to detect possible cases of tax evasion and/or money laundering involving identity fraud?

16. Several "red flag indicators" are used by tax authorities to detect possible cases of tax evasion and/or money laundering involving identity fraud. These indicators are outlined below in six categories:

Geographic - Address/Location:

- Address used to facilitate the identity fraud.
- Address of the suspected person.
- Use of common address and bank accounts by several people and corporations.
- Client filing returns in different regions of the country.
- Post Office Box addresses being used, or the use of non-existent addresses, e.g., residence, employer address, etc.; or the postal code for the client or employer is not consistent with the address given.
- Business not located where person lives.
- Tax refunds posted to same address.
- Tax refunds sent to post office/mail boxes rather than a real address.
- Tax refunds mailed to address other than that listed on tax return as residence of taxpayer.
- Tax refunds are being sent to return preparer's address.

Financial Analysis:

- Value of tax refund or rebate.
- Large unusual claims and deductions, or similar claims all made in the same manner or format.

- Income appears unreasonable for the client; e.g., first year filer; tax deducted unusually high for earnings reported.
- Excessive deposits whose origins are not justified.
- Acquisition of luxury transport means.
- Under invoicing on real estate sector.
- Analysis of Suspicious Activity Reports (SARs) indicating the use of several bank accounts receiving large deposits from different sources.
- Tax withholding amounts are much larger than would be appropriate for amount of income earned.
- Insufficient income to start a business.
- Transactions involving tax havens.

Documentation and Business Operations:

- Similar typing, handwriting, addresses, signatures, format, refund amounts.
- Apparently unrelated returns all packaged the same.
- Same staples/paper clips used, and/or inserted in similar places on the return and/or the Order of Attachments is the same.
- Same discounter used on multiple returns. This may imply collusion or possible scheme by discounter or employees.
- Signatures on duplicate returns appear different.
- Receipts of any kind appear to have been written or altered by client or tax preparer.
- Income tax source deduction slips for different employers apparently prepared by the same individual (e.g. same handwriting, or with the same typewriter or computer printer).
- No employer identification on income tax source deduction slips, or curious/odd looking employer names.
- income tax source deduction slips filed by client is prepared differently from other deduction slips filed by the same employer.
- Information slips appear altered.
- Companies that do not report income but have performed transactions reported by third parties.
- Communications of the control financial authorities and public notaries to the tax administration.
- Use of nominees and the use of corporate vehicles to hide behind.

Individual Characteristics, Identity, Behaviour and Associations:

- Residency status of suspected person(s).
- Association with certain tax agents.
- Compliance history of suspected person(s).
- Group of clients in the same age group.
- Tax Identification Numbers (TINs) in the same range; e.g. TINs beginning with the same first 3 digits.

- Similar style family names on a group of returns, e.g. White/Black/Green or Anderson/Sanderson/Henderson.
- Group of clients with different employers but in the same profession.
- Multiple referrals with same employer.
- Suspected person possibly too young or too old to start a business.
- Contact purported registrant and they claim not to know anything about the business.
- Taxpayers that cannot recognize or properly explain the operations associated with them when questioned by tax auditors.
- The repeated loss of an identity card (several times a year)
- Taxpayers that cannot recognize ownership of relevant bank accounts.

Timing

- Multiple numbers of returns filed simultaneously, or dated on and around the same date.

Other:

- Some level of detection may be derived from requests for information made in unusual circumstances, e.g. illegal approaches by bogus HMRC officers relating to a tax or lottery-related issue.
- Social Security number placed on tax returns does not match Social Security Database.
- Multiple returns are filed with variations of the same Social Security Numbers (Scrambled SSNs).

Information sources available to tax authorities to assist in the detection and investigation of cases involving tax evasion and money laundering involving identity fraud.

17. Most of the countries surveyed use multiple sources of information, available within and external to their tax authority, to detect and investigate possible cases of tax evasion and/or money laundering involving identity fraud. Effective information sharing between tax authorities and other domestic agencies is also crucial to detecting and investigating such cases.

18. Examples of useful sources of information available within or obtained by tax authorities for such purposes include:

- Information contained in tax returns.
- Real estate transactions and mortgage loans/mortgage loan agreements performed by a Notary Public.
- Printing jobs undertaken by printing houses authorized by the tax authority.
- Registers' information on real estate, aircraft and vessels.
- Transactions performed by agents of foreign non-resident taxpayers and/or reported by third parties in the transaction.
- Birth registers, driver licence registers etc.
- Employer records.
- Financial institution records.
- Open source information (e.g. telephone records, Internet, newspapers, etc).

- Disclosures from Financial Intelligence Units (FIUs).
- Spontaneous exchange of information received from other States; and
- Credit reference agencies.

19. Several countries reported that their tax authorities have arrangements with other government and third party agencies [e.g. Memoranda of Understanding (MOUs)] to exchange information on relevant matters. Such other government institutions include social security, customs and immigration agencies; driver's licence and birth registrars; police and other law enforcement agencies; overseas tax authorities; postal services and trade commissions.

Examples of information used to detect and investigate identity fraud, including information sharing arrangements between tax and other domestic law enforcement agencies

In **Australia,** tax authority records, external government agency records (birth registers, driver's licence registers etc), employer records, financial institution records and open source information (telephone records, Internet etc) are used to detect and investigate suspected identity fraud cases. Tax authority records are used to check the status of the taxpayer and their tax refund claim history. External records are used to determine the validity of the identity of the person filing tax returns. Employer records are used to determine the validity of claims. Open source information is used for a variety of purposes, including determining the veracity of the claim and the identity of the client. The Australian Taxation Office has legal and contractual (MOU) arrangements with Centrelink (welfare agency), Immigration, Driver Licensing and Birth Registrars, as well as with law enforcement agencies including the Australian Crime Commission's Australian Identity Protection Register.

In **the United Kingdom**, information is sought to both assist the investigative process and to obtain evidential information to use within the prosecution. Information obtained is analysed for relevance and may lead to further investigative enquiries that will involve attending court to obtain production orders or search warrants and /or restraint action against assets identified or believed to exist. Information is used to build up the case for an arrest and eventual prosecution through the court. HM Revenue and Customs has a particularly close relationship with DWP (national benefits authority) and it shares data through a number of established legal gateways, including for investigating and prosecuting offences relating to social security, employment and training. HMRC also participate in a regular cross-government forum, with private sector representation, which discusses identity fraud issues.

How countries investigate cases of suspected tax evasion and money laundering involving identity fraud (including multi-agency cooperation)

20. Several countries report that their tax authority investigates cases of identity theft/fraud either independently or in partnership with other law enforcement agencies (including FIUs). In **Australia**, tax agents and communications carriers also play an important role in the detection of perpetrators. In **Canada**, some tax officials are seconded to Integrated Proceeds of Crime (IPOC) units that investigate such offences. In order to combat the underground economy and organised crime more effectively, **France** has put in place regional task-forces (*Groupes d'Intervention Régionaux, GIR*). These are staffed by police and customs officers, the *gendarmerie*, tax inspectors and personnel from the competition and anti-fraud directorate and from URSSAF (social security). In **Germany**, if tax audits reveal grounds to suspect identity fraud (or money laundering), the prosecuting authorities are informed and they may then conduct searches / seizures as necessary. If when conducting searches/seizures because of tax evasion the tax investigation service finds documents which point to identity fraud (or money laundering), these are handed over to the prosecuting authorities for further action. In **Ireland**, the tax authority and social welfare agency have joint investigation units that facilitate investigations. In **Mexico**, the methods and strategies used to investigate tax evasion cases involving identity fraud include requesting bank account(s)

information to certify and verify the account holder's identity, data-matching with other information to verify identity, collaborating with other government agencies and tracking cash flow.

Case studies dealing with multi-agency cooperation to investigate cases involving tax evasion and/or money laundering involving identity fraud

Australia: The Australian Taxation Office (ATO) investigate this class of crime, either independently or in joint operations with its partner law enforcement agencies the Australian Federal Police and the Australian Crime Commission. AUSTRAC (the Australian Financial Intelligence Unit), financial institutions, tax agents and communication carriers also play an integral role in the detection of perpetrators. The ATO has a rapid response capability to quickly test and close exposure in a wider context, and to address systemic or control failures. The armoury of physical and technical surveillance, computer and accounting forensics, and on occasions, coercive questioning available to the Australian Crime Commission is used to meet these challenges. Proceeds of Crime forfeiture provisions are also used effectively to recover assets. The Commonwealth Director of Public Prosecutions prosecutes all tax related fraud and can play a role throughout the investigative process.

Spain: When the clues indicate that there is an important case of tax fraud and money laundering, the tax authorities contact the police and prosecutors to examine the case and implement techniques such as intercept phone calls, pursuit or surveillance of persons, etc.

Sweden: The Swedish Tax Agency has no authority to combat money laundering on its own. The strategy is to a large extent to cooperate with other agencies. A structure for cooperation is being built up for the moment including the Finance police, the Economic Crime bureau, the National Prosecutor, the regulatory agency Finance inspection, the Company Registration Agency and the Swedish Customs. So far the cooperation has mainly been between the Finance police and the Tax Agency.

United States: IRS-Criminal Investigation (IRS-CI) is the only US agency authorized to conduct criminal tax investigations. For money laundering investigations IRS-CI will work with the other US law enforcement agencies that will have jurisdiction over the predicate crime which can include FBI, Federal Trade Commission, Social Security Administration, and US Postal Service. For example, the Identity Theft Task Force (IDTF) is a nationwide strategy being implemented to combat ID Theft and Fraud initiated by the President in 2006 that will join the efforts of the aforementioned agencies and others.

Effective measures undertaken by tax and other government agencies to increase compliance and deter non-compliance regarding identity fraud

21. Several of the countries surveyed reported that they have implemented a range of strategies that have proven effective to reduce the opportunity to commit tax fraud and/or money laundering that involved identity fraud. Effective strategies in this regard generally involve a mixture of data mining, data matching, risk profiling, inter-agency cooperation, training and public education.

22. In **Argentina**, **Australia**, **Canada**, **Ireland**, **Mexico**, the **United Kingdom** and the **United States**, marketing and education campaigns have been introduced to alert the public about the risks associated with identity theft and identity fraud. In **Germany**, in recognition of the fact that most cases of tax fraud/money laundering are detected by the tax investigation service or by the field audit units, extensive training is given to the tax investigation units and the field audit units. In **Japan**, the Law on Customer Identification and Retention of Records on Transactions by Financial Institutions requires financial institutions to handle customer's identification and to keep records of their transactions by making a contract with their customers. In December 2004, the Law on Customer Identification and Retention of Records of Transactions by Financial Institutions was amended to avoid the abuse of bank accounts. In **Mexico**, training courses or workshops are delivered to persuade and guide reporting entities with regard to their AML/CTF obligations. One of the important obligations in this regard is proper

identification of customers and users. In **Turkey**, the Unique Identity Number (UIN) is being used in most public services such as health and education. The UIN is also being used as the tax identification number.

Examples of measures undertaken by tax and other government agencies to increase compliance and deter non-compliance regarding identity fraud, including education and other awareness campaigns.

Argentina: The tax authority has strengthened mechanisms to counter the use of false invoices involving fictitious individuals or corporations to simulate transactions designed to reduce taxes payable. This highly effective strategy requires taxpayers that file for VAT registration to submit prior evidence of certain wealth that ensures a degree of certainty regarding their actual existence. The fraud cases detected have been disclosed via the mass media (newspapers, radio and television). The tax authority has also undertaken an ongoing tax education campaign, from elementary school onwards.

Mexico: The competent authorities undertake public campaigns, warning taxpayers not to use false invoices or to engage in activities with networks of companies that have been already detected. These campaigns aim to increase the risk perception among taxpayers. Additionally, reporting entities have preventive controls as regards money laundering, terrorism and its financing, to reduce the possibility of criminals hiding the illicit origin of their resources. The authorities provide training courses and workshops to persuade and guide reporting entities with regard to their AML/CTF obligations. One of these obligations is the proper identification of customers and users.

United Kingdom: HMRC, along with other government departments, is contributing and participating in the marketing communications campaign being spearheaded by The Identity Fraud Consumer Awareness Group (IFCAG). This group (which is composed of public and private sector organisations) has the following objectives: (1) to promote anti-fraud measures to the general public and work that both the public and private sector can do to protect their own systems; (2) to promote understanding of identity fraud/ theft and what steps victims can take to protect themselves; (3) to develop, launch and maintain an Internet site to disseminate essential information on identity fraud/theft to the public; (4) to develop and take forward a series of wider consumer awareness campaigns through non-Internet channels; and (5) to develop and implement a marketing and communications campaign to further raise public awareness of identity fraud.

Results of activities designed to detect and address non-compliance, and to promote compliance

23. Most countries surveyed reported that it is difficult to measure the results of their tax authority's compliance activities over the last three years in terms of detecting and investigating tax fraud and/or money laundering in cases that involve identity theft and identity fraud.

24. In **Argentina**, there has been a reduction in the level of non-compliance and an increase in tax and social security revenues. In **Australia**, there have been a greater number of cases detected and a significant amount of money has been saved. In the **United Kingdom**, HMRC has realized significant achievements in combating fraud since the introduction of tax credits. During 2005-06, HMRC prevented three quarters of all attempted organized fraud that had been identified, protecting £409 million in payments. In **the United States**, during the 2006 financial year (as of April 30, 2006) the IRS-CI division has 95 cases involving identity theft under active investigation, and 106 cases are completed and awaiting legal review or prosecution. The average sentence received in identity theft cases is 42 months.

Examples of successful activities designed to detect and address non-compliance and to promote compliance regarding identity fraud

Mexico: During the period January 2005 to August 2006, 1089 letters of invitation were sent to unlicensed reporting entities, in order to warn and inform them about the criteria, measures and procedures of the customer due diligence regarding identification. By September 2006, 52% of the letters of invitation were answered, and taxpayers provided

the required documentation about the due fulfillment of fiscal obligations. Additionally, during this period, 451 inspection visits were made to supervise the operations of taxpayers.

United Kingdom: HMRC has an active strategy to tackle tax credits fraud. HMRC has realized significant achievements in combating fraud since the introduction of tax credits. During 2005-06, HMRC prevented three quarters of all attempted organized fraud that has been identified, protecting £409 million in payments. Through its compliance operations, in 2003-04 HMRC intervened on over 1,800 incorrect claims where a false or fraudulent claim was suspected before tax credit payments were made. In 2004-5 this increased to 17,000 and in 2005-6 it increased again to around 100,000. 193 individuals were successfully prosecuted for tax credit fraud in 2004-05. In 2005-06 responsibility for prosecuting individuals in England and Wales passed to Revenue and Customs Prosecution Office (RCPO). RCPO and the prosecuting agencies in Scotland and Northern Ireland prosecuted 188 individuals in 2005-6 for tax credit fraud. The slight reduction on 2004-05 figures indicates a realignment of HMRC's resources in 2005-06 to tackle more cases of organized fraud. Furthermore in 2005-06 HMRC imposed 2,241financial penalties with a total value of around £900,000.

United States: The following table provides IRS-CI identity theft statistics for the past 4 years:

	FY 2002	FY 2003	FY2004	FY 2005
Cases Initiated:	80	102	96	70
Sentencings:	13	11	26	25