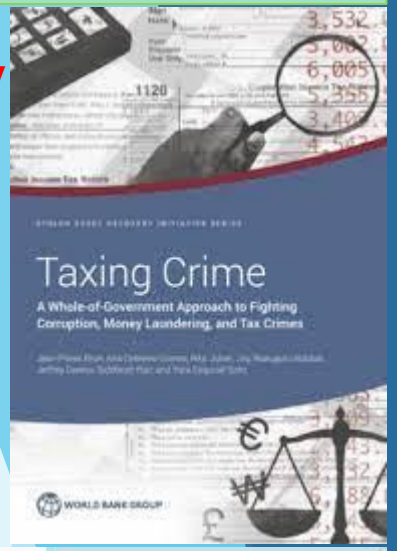
TRADE BASED MONEY-LAUNDERING

and ELECTRONIC SALES SUPPRESSION

(Introduction)

Sometimes the figures just do not ad up, there is no escaping the accounting world of debits and credits.

THE THREE UGLY SISTERS : TAX EVASION + ML AND IFF'S



The cash economy and cash used in TAX EVASION schemes are in many instances inseparably linked to MONEY LAUNDERING and ILLICIT FINANCIAL FLOWS

- A **crime** is an illegal or unlawful activity, a violation of a law in which there is injury to the public or a member of the public and a term of jail or prison and or fine or penalties exists (Smith, 2012).
- The definitions of **tax evasion** and **crime** indicate that both are illegal practices.
- Another characteristic that can be derived from the definitions of tax evasion and crime is that by evading taxes there is 'injury' to the public.

The commonalities identified by comparing the definitions of TAX EVASION and MONEY LAUNDERING :

1. both are unlawful activities;
2. both involve the violation of laws;
3. the acts are **deliberate** in both tax evasion and money laundering; and
4. both of these offences disguise or conceal the money received.

Why criminals launder money - some reasons :

- Trying to **hide wealth**;
- they want to **evade taxes** in order to **increase their profits**;
- they want to **legalize the money** and they want to **avoid prosecution**.

➢ ***The problem : Declaring illegal funds for tax purposes will risk being prosecuted for the offence of money laundering and/or other applicable offences.***

ILLICIT FINANCIAL FLOWS - The **cross-border movement of money** that is illegally earned, transferred, or utilized, is referred to as the flow of illicit funds (Renner, 2012). This usually involves the transfer of money earned through illegal activities, for example criminal deeds (money laundering) and corruption, as well as efforts to hide wealth from a country's tax authorities.

= Deriving from this explanation of illicit financial flows, it can be stated that the offences of both money laundering and tax evasion are included in illicit financial flows.

Trade based Money Laundering and taxation

Trade-based money laundering is defined as the process of **disguising** the proceeds of **crime** and moving value through the **use of trade transactions** in an attempt to **legitimize their illicit origins**. In practice, this can be achieved through the **misrepresentation of the price, quantity or quality of imports or exports**. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further **obscure the money trail**.

There are **three main methods** by which criminal organisations and terrorist financiers move money for the purpose of **disguising its origins and integrating** it into the **formal economy**.

- The first is through the **use of the financial system**;
- the second involves the **physical movement of money** (e.g. through the use of cash couriers); and
- the third is through the physical movement of goods through the trade system

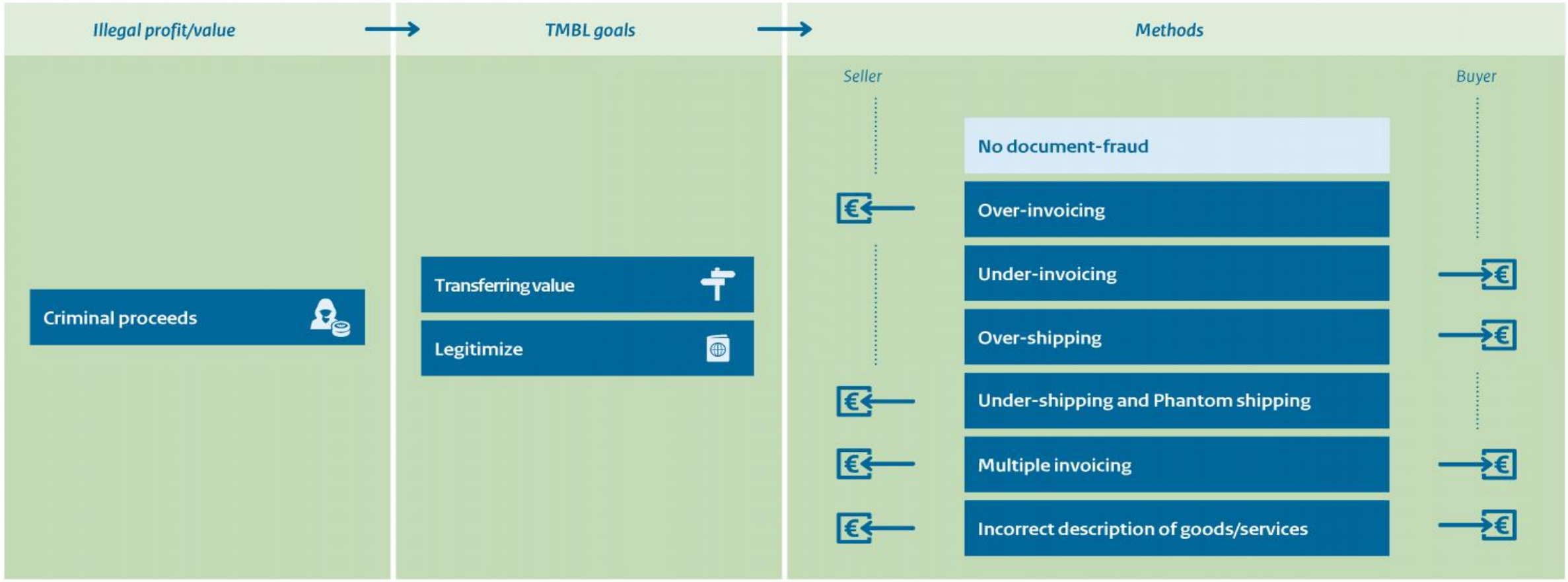
Tax evasion as a predicate offence for money laundering

Money Laundering is a three-stage process

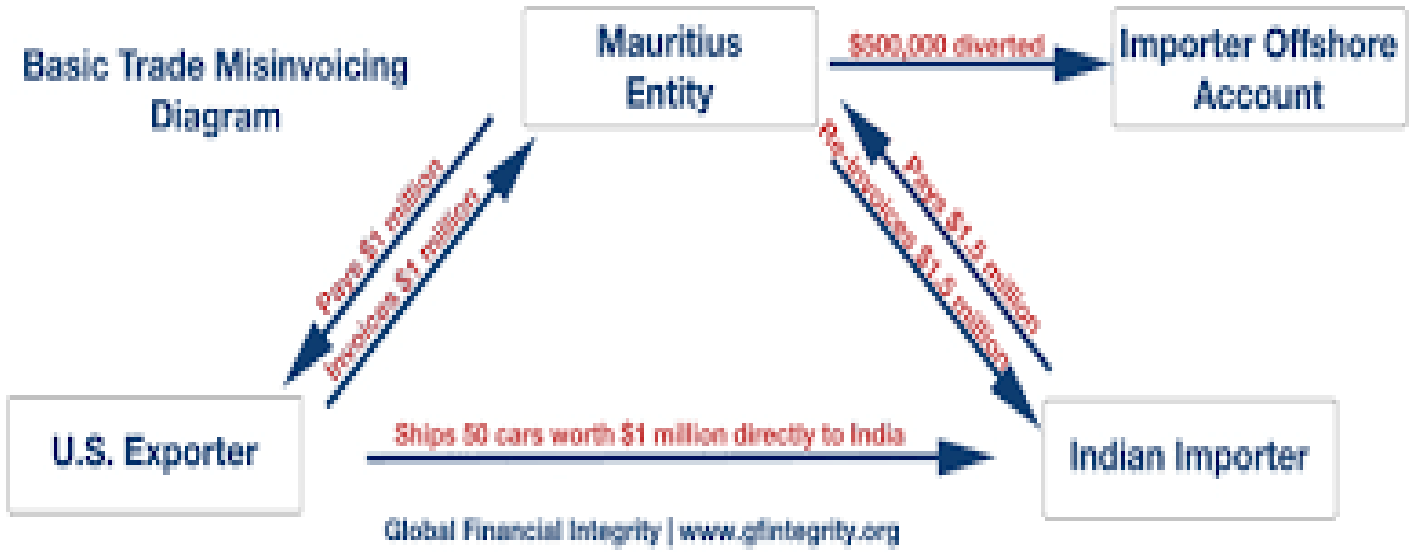
1. which starts with the money coming from the crime first being placed somewhere to hide its link to the crime **(placement)**.
2. After it has been placed it is layered, which means its connection to the crime and the criminal is further disguised. This can be done, for example, by a series of transactions, a process which often involves the **money being transferred through several banks abroad** or being used to set **up shell companies in tax havens (layering).**
3. After it has been layered successfully, the money (which can also be in the form **of property**) is then integrated into the lawful economy **(integration).**

- It is a good habit now and then to question things that one has taken for granted for years. - German proverb

DETECTING TRADE BASED MONEY LAUNDERING – NETHERLANDS AMLC



EXAMPLE TRADE BASED MONEY LAUNDERING



US EXPORTER	
Invoice Mauritius Company	$1,000,000
(No VAT - direct export)	
MAURITIUS COMPANY	
Cost - Receives Invoice and pay US Exporter	-$1,000,000
Revenue - INVOICE Indian Importer - No VAT	$1,500,000
Profit in low tax jurisdiction	**$500,000**
INDIAN IMPORTER	
COST - INVOICE Indian Importer	$1,500,000

HOW BIG IS THE PROBLEM – EVERY YEAR

Globally

According to reports from UNODC and Europol, **2% to 5%** of the **global GDP** is **laundered every year** = This accounts for **EUR 715 billion to EUR 1.87 trillion.**

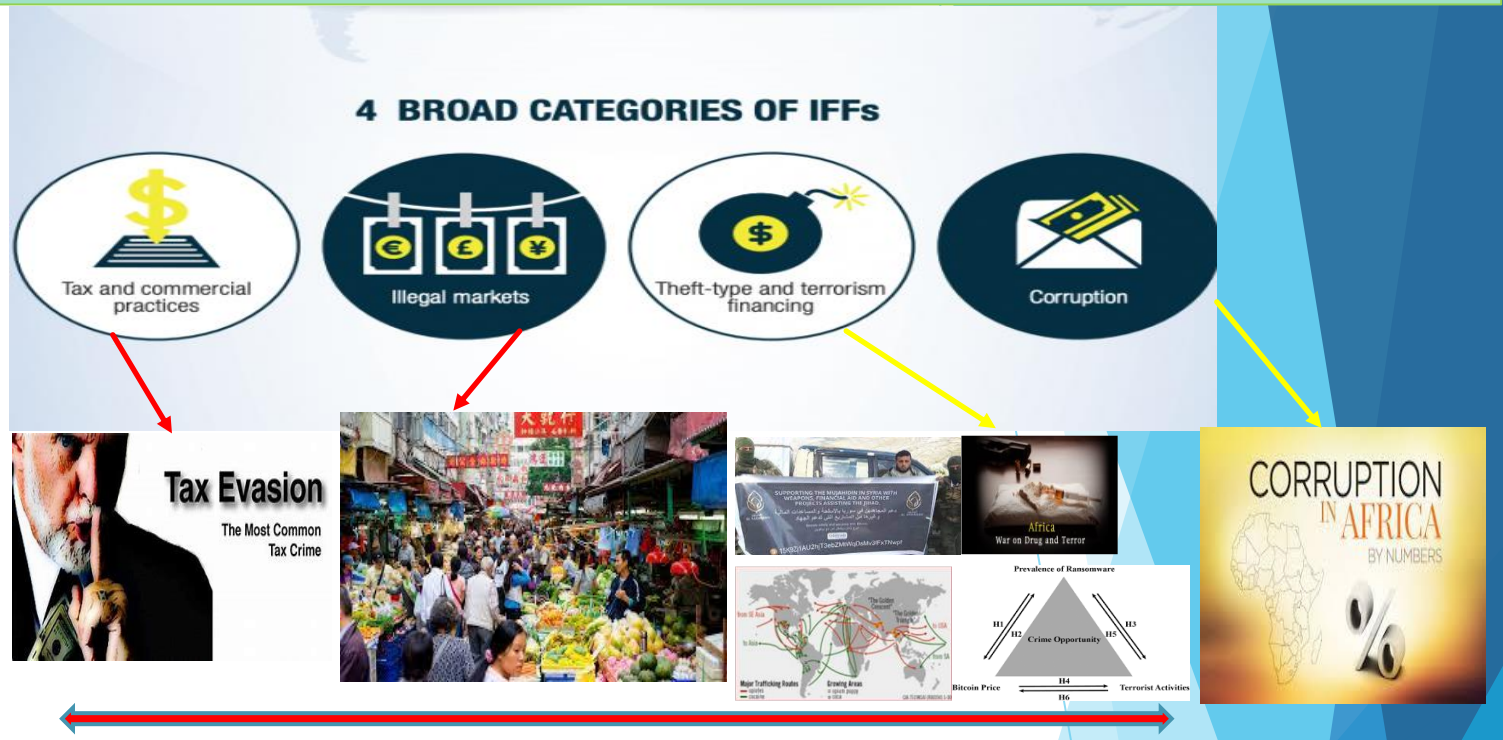
African continent

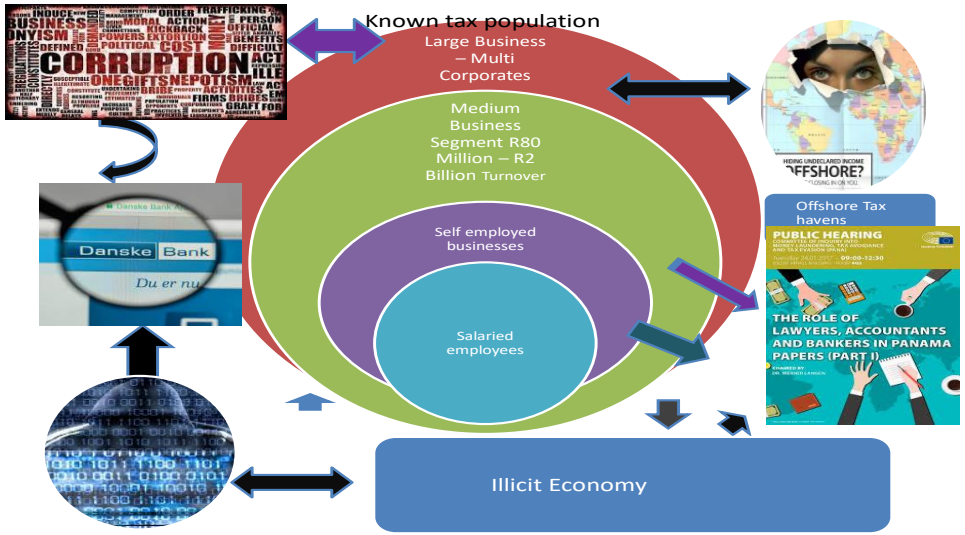
According to the Economic Development in Africa Report 2020 by the UN Conference on Trade and Development (UNCTAD) :

Africa loses about US$88.6 billion, 3.7% of its gross domestic product (GDP) annually in illicit financial flows.

Curbing IFFs, according to UNCTAD, could almost **halve the $200 billion annual financing gap Africa** faces to achieve the sustainable development goals (SDGs).

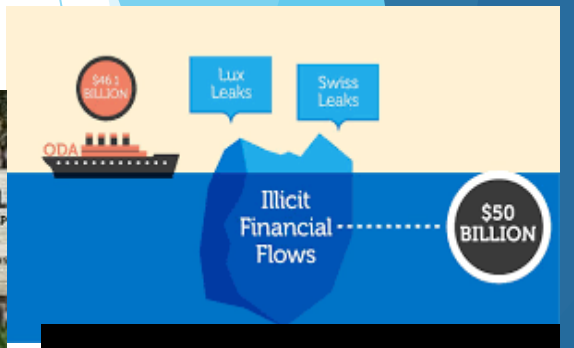
= Money-laundering is not a victimless crime and the life support system for financial crimes

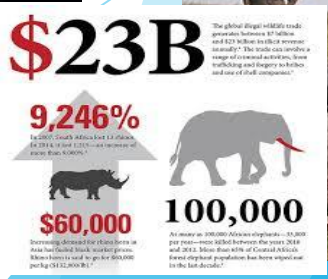




EXAMPLES OF MOVING ILLICIT FUNDS

- **TRADE BASED MONEY LAUNDERING** – price and invoice manipulation
- **BULK CASH SMUGGLING (Cash Mules)** - depositing it in a financial institution, such as an offshore bank, that offers greater bank secrecy (Gold, diamonds, currency)
- **HAWALA NETWORKS** – hawala brokers, or hawaladars. It is the transfer of money **without actually physically** moving it
- **CASH INTENSIVE BUSINESSES - uses its legitimate accounts to deposit criminally derived cash**
- **ATTORNEY TRUST ACCOUNTS** (Panama, Paradise and Pandora leaked papers)
- **PURCHASE OF LISTED SHARES and SECURITIES** – local and international indexes
- **PURCHASE OF PROPERTY** : fixed property, jewellery, artwork
- **CASINOS and GAMBLING**
- **CRYPTOCURRENCY and E-wallets**
- **RELIGIOUS ORGINISATIONS** – contributions, books and on-line services
- **LEGAL and ILLEGAL WILDLIFE TRADE**
- **BANK CAPTURE** - money launderers or criminals buy a controlling interest in a bank
- **PURCHASE OR SPONSORING SPORT TEAMS/CLUBS**
- **ONLINE ADVERTISING**
- **INSURANCE POLICIES** with termination date
- **COMPLEX TAX STRUCTURES**
- **LOW TAX JURISDICTIONS** – profit shifting
- **BANK SYSTEM FRAUD** - smurfing, is a method of placement whereby cash is broken into smaller deposits
- **SHELL AND FRONT COMPANIES** – Beneficial ownership
- **BACK TO BACK LOANS**





BULK CASH SMUGGLING – CASH MULES – HAWALA NETWORKS

11 September 2015

Five people were arrested at OR Tambo International Airport after being found with **undeclared currency totalling R23m**, **as well as a further $3.77m (R50.2m)**. The passengers were scheduled to leave South Africa on United Arab Emirates flight to Dubai cash was hidden in 12 pieces of luggage, including four backpacks.

Two sources, independent of each other, have said the agencies believe the money was on its way to Pakistan. They also believe some of the money was destined for the self-proclaimed Islamic State (Isis).

Publication: NEW AGE, THE
Date: 2015-09-11
Page: 1

'BILLIONS FLY OUT'

SARS GIVES RESERVE BANK R78M FROM FIVE DUBAI-BOUND 'MONEY CARRIERS'

VUSUMUZI SHABANGU

MASSIVE amounts of South African and foreign currency are being smuggled out of the country via OR Tambo International Airport on a regular basis.

The currency smuggling known as hawala came to light last week when five men boarding a flight to Dubai were intercepted by customs officials with undeclared currency of R78m which included US dollars.

The South African Revenue Service (SARS) said the suspects were attempting to board with eight luggage cases and four backpacks.

SARS said the money seized was handed over to the SA Reserve Bank for further investigation.

The suspects have not appeared in court. Sources, however, told The New Age the money seized was the "tip of a very large currency smuggling iceberg".

"The men arrested were the runners for one of six or seven operating syndicates involved in hawala. To avoid paying corporate and sales tax, business people in the Indian, Chinese and expatriate communities launder money by smuggling it out."

The source said the courier syndicate busted would undertake between two to three trips a week.

"The R78m seized seemed exceptional. My understanding is that the currency regularly smuggled amounts of R20m, on average, on each trip. With six or seven syndicates in operation, you do the sums. Billions of rands are flowing out of the country annually." The source said the courier syndicates charged their clients 4% on the amount smuggled.

"These are people who are simply skimming cash out of their tills to avoid taxation and who are keen to invest it off-shore.

"This is not round-tripping of laundered money. It never comes back but is invested in property or businesses elsewhere."

Dubai seems to be the favourite destination for hawala.

"Couriers truthfully declare the currency amounts they are carrying on arrival at Dubai airport where customs officials provide them with paper work to be presented at local banks. It's deposited into the off-shore accounts of their South African clients."

The source said the currency smuggling was facilitated by corrupt customs officials.

"I'm aware of entire consignments of cash being seized by customs and never declared to the authorities. Customs jobs at OR Tambo is apparently highly sought after."

However SARS spokesperson Sandile Memela said there was no evidence that pointed to SARS officials colluding with syndicates to move money out or undermine law enforcement.

"All the cash that has been seized was handed over to the South African Reserve Bank for further handling," he said.

The police had not responded at the time of going to press.

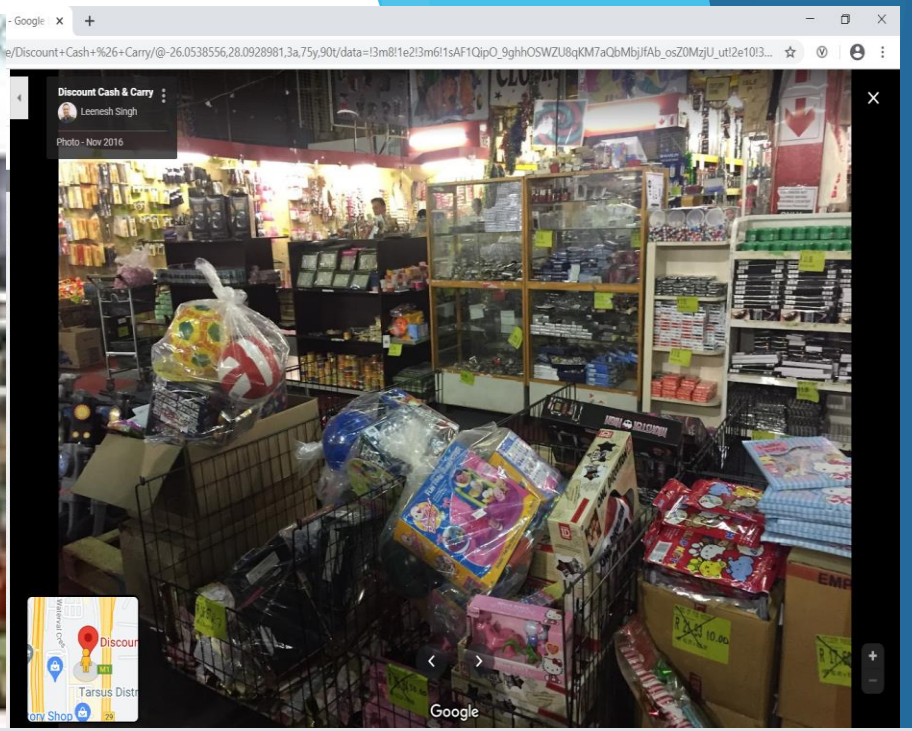
vusmzis@thenewage.co.za

Hawala – money smuggling at new level

- Five men intercepted at ORT, R78m seized
- 6 to 7 hawala syndicates are known to operate
- A means for local business people avoid paying taxes
- Syndicate could make three trips a week
- Couriers carry an average of R20m on each trip
- 'Clients' are charged 4% of the amount smuggled
- Dubai is a favourite destination. Lax banking system
- Smuggled cash invested in UAE
- Customs officials allegedly complicit

EXAMPLE 1 –
WHAT POTENTIAL RED FLAGS DO YOU OBSERVE

EXAMPLE 2 - WHAT POTENTIAL RED FLAGS DO YOU OBSERVE



EXAMPLE 3 –
WHAT POTENTIAL RED FLAGS DO YOU OBSERVE

Hyatt Hotel Data			
Hotel	**Cash Rate**	**Points Rate**	**Cash + Points Rate**
Grand Hyatt New York (New York, New York)	$868.04	80,000 (valued at $1,520)	$470.70 + 40,000 points (total value $1,230.70)
Hyatt Place Charlottesville (Charlottesville, Virginia)	$455.32	32,000 (valued at $608)	$284.57 + 16,000 points (total value $588.57)
Hyatt Place Moab (Moab, Utah)	$676.06	32,000 (valued at $608)	$422.54 + 16,000 points (total value $726.54)
Hyatt Palm Springs (Palm Springs, California)	$1,298.73	48,000 points (valued at $912)	$739.67 + 24,000 points (total value $1,195.67)
Hyatt Regency Maui (Lahaina, Hawaii)	$1,570.74	100,000 (valued at $1,900)	$1,036.62 + 50,000 points (total value $1986.62)

Calendar Start Period — Wednesday, March 1, 2017

Total # of Room — 55 — edit room information

Status Code — 5

Ucode	No	Status Name	Description
B	1	Booked	
S	2	Stayed	
X	3	Cancelled	
MR	4	Booked - Move Room	
URM	5	Under Renovation/Maintenance	
	6		
	7		
	8		
	9		
	10		

account ageing report

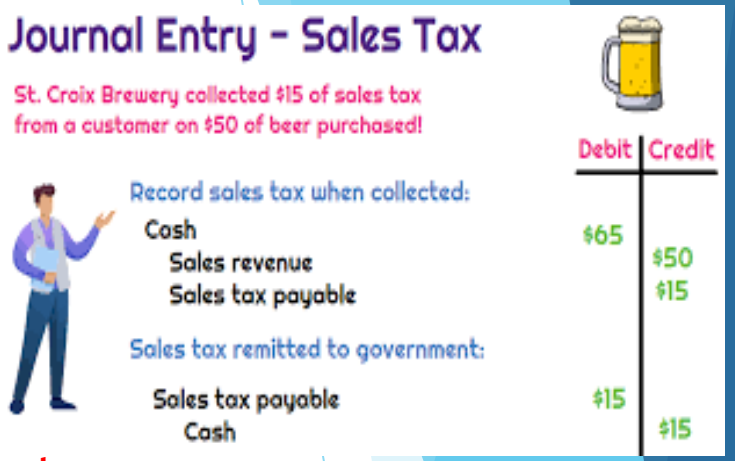
Aged Accounts receivables as on : Sr. No.

			Outstanding (in days)				
Name	**Balance**	**Current**	**Upto 30**	**31-60**	**61-90**	**91-120**	**120+**
Mr. J	6488.60		6488.60				
Mr. B	15365.00						15365.00
Mr. C	9575.00	4000.00	5575.00				
Total outstanding	31428.60	4000.00	12063.60				15365.00

ELECTRONIC SALES SUPPRESSION (ESS) AND TAX EVASION

WHEN IS SALES TAX PAYABLE – GENERAL RULE

Sales tax or VAT is not part of business's "profits"



- ✓ The end-user becomes liable for taxes (VAT/GST) on the payment
- ✓ for goods or services
- ✓ to the shop owner/vendor company
- ✓ collecting on behalf of the State
- ✓ being liable to honest and fully declare receipts and pay over taxes collected in fiduciary role

Sales tax vs. VAT overview

Sales tax is collected by the retailer when the **final sale in the supply chain is reached**. In other words, end consumers pay sales tax when they purchase goods or services. When buying supplies or materials that will be resold, businesses can issue resale certificates to sellers and are not liable for sales tax. Until the sale is made to the final consumer, sales tax is not collected, and tax jurisdictions do not receive tax revenue.

VAT, on the other hand, is collected by all sellers in **each stage of the supply chain**. Suppliers, manufacturers, distributors, and retailers all collect VAT on taxable sales. Similarly, suppliers, manufacturers, distributors, retailers, and end consumers all pay VAT on their purchases. Businesses **must track and document the VAT they pay on purchases** to receive a **credit for the VAT paid on their tax return**. Under **a VAT regime**, tax jurisdictions receive tax revenue throughout the entire supply chain, not just at the point of sale to the final consumer.

WHY A CASH REGISTER

What is a Cash Register

A cash register (also known as a “till”) is the machine used by businesses to calculate and record **financial transactions,** it has a keypad used to input values

A machine used in shops has a drawer for receiving cash money and

- **total a sale,**
- displays the sale and
- records the **amount of each sale and sales for the day**

The newer and more modern cash registers functionalities include attachment points for a

- barcode scanner
- receipt printer and
- scales (weighing items)

How did a cash register evolve

Invented in 1879 and patented in 1883 by saloonkeeper James Ritty, the seen-everywhere cash register — still called a “till”

Necessity bred the invention of the cash register: his saloon employees **failed to bank deposit all cash sales** at the Manhattan and San Francisco bars that managed to still be **“cash-only.”**

Dubbed the **“Incorruptible Cashier,”** Ritty’s invention made it possible for business owners to worry a little less about **skimming.** The first cash register was called the Ritty Model I and H. Eckert of Cincinnati, Ohio purchased the patent adding a few more features to be marketable :
a cash drawer and **tweaked the bell,** which now served a dual purpose: **Notifying managers the cash register was being opened** and giving customers a pleasant sound that enhanced, and tied itself to, the in-store experience.

ELECTRONIC POINT OF SALE SYSTEM (POS)

Cash register is a simplistic way to **receive sales transactions**, hold money, calculate tax, **print receipts**, and give change to your customers – relatively easy to operate and cheap to purchase and maintain.

Point-of-Sale (POS) system : an **advanced version of the cash register**. It can do all the basics like a cash register more effectively with features like :

- inventory control,
- real-time data reporting and analysis,
- employee monitoring and
- generating various reports – including exception reports

- Modern POS systems are **commonly programmable** or allow enhancement with third-party software programs.
- These systems **can be tailored to meet specific needs**. For example : many retailers use POS systems to **manage membership programs** that **award points to frequent buyers** and **issue discounts** on future purchases.
- Cloud-based **POS systems** are increasingly in use, particularly for **large online merchants**, to track and process numerous purchases. Cloud-based systems can greatly reduce the upfront costs of implementing a POS system for many businesses.
- **Customers can also interact directly with POS systems**, particularly in the hospitality industry – placing orders for room service or to pay hotel bills

MODERN POINT OF SALE DEVICES

- Many supermarket chains today have **self-checkout devices.**
- **Customers scan the barcodes, pay by cash or card, and bag their shopping.** They do all this without any intervention from the staff. A staff member is available in case you need help.
- Employees are also at hand to check customer's ID. They need to make sure customers are old enough to buy some products. For example, if you want to buy alcoholic beverages, the employee needs to approve the sale.

WHAT COULD POSSIBLY GO WRONG – automatic 'magic' accounting?

LATEST SMARTPHONE PAYMENT METHODS

Zapper payment applications - Smartphones

- Zapper allows your customers to pay using their smartphone without having to call the waiter back to the table.
- Zapper even supports splitting the bill. Place the Zapper QR Code anywhere - in emailed PDF bills or printed invoices. Customers scan the QR Code and supplier is paid in seconds. (Total invoice incl VAT/GST)
- With Zapper you can pay bills in a matter of seconds and quickly log in and sign up to websites, without using a keyboard.
- Zapper includes an online dashboard. This allows you to select the services you need, monitor activity and reconcile payments. So whatever Zapper service you use, you'll have insight into activity.
- Payments are quick, secure and effortless and the **business spend less time and money taking payments and chasing up invoices**. Cash flow improves, sales increase, costs decrease and customers enjoy buying experience.

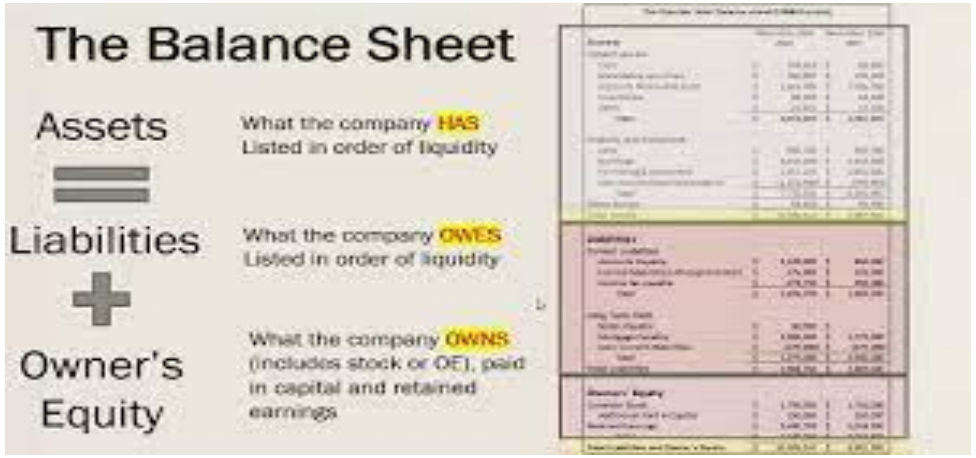
HOW are these sales recorded in the business accounting records? and/or

HOW are these incorporated in accounting records ?

Should the business be registered for VAT ?

POS POSSIBLE CONFIGURATIONS, DATA AND ACCOUNTING

≠



How is POS Software different from Accounting Software?

POS saves **data**
POS software options with **"integrated"** and **"interfaced"** options

Two types of accounting approaches

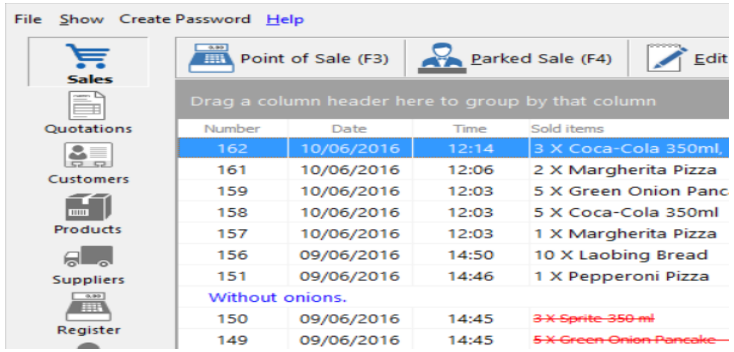
Integrated modules rely upon the dame3 data files, while information(data) is updated in **real time**. Maximum integrity is achieved through the **consistent data preservation across all modules**. This also prevents wasting time and the possibility of **double-entries.**

Interfaced modules, on the other hand, **use software with established protocols** that can effectively translate and then transfer data back and forth. Most of these interfaces are designed to communicate with **third party programs.** The **interface requires manual manipulation** and it **does not occur in real-time.**
Some POS system that comes with **fully integrated accounting** built into the software, or the client could prefer to work with accounting software like : Pastel, QuickBook, Peachtree, etc.

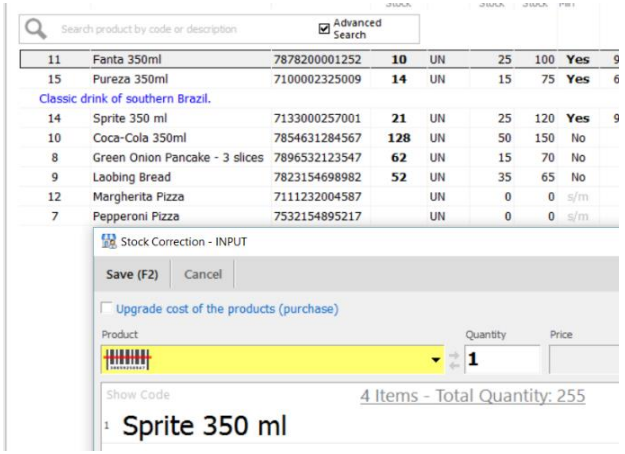
LOOK AND FEEL OF POS POSSIBLE REPORTS – SALES AND STOCK

- **POS data** may be used to create a **large number of reports** - the **data will be contained on storage devices, servers or via cloud**
- The **original core data integrity** is **arguably sound** given the POS software design (**unless destroyed)**
- **HOWEVER,** the **structure of the POS reports** and data ***fields used*** ***to extract data*** for any report is **susceptible to manipulation.**

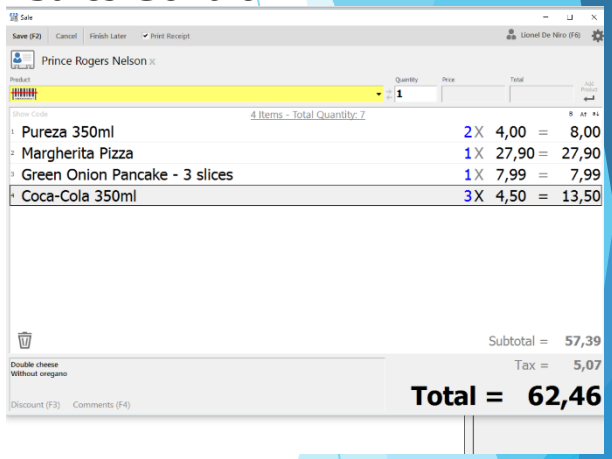
Main Screen



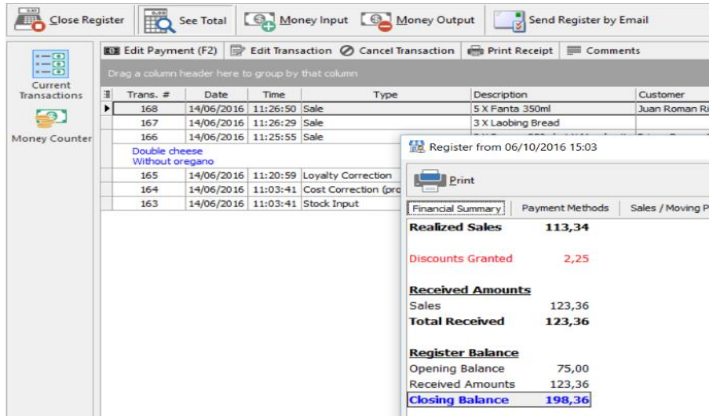
Inventory



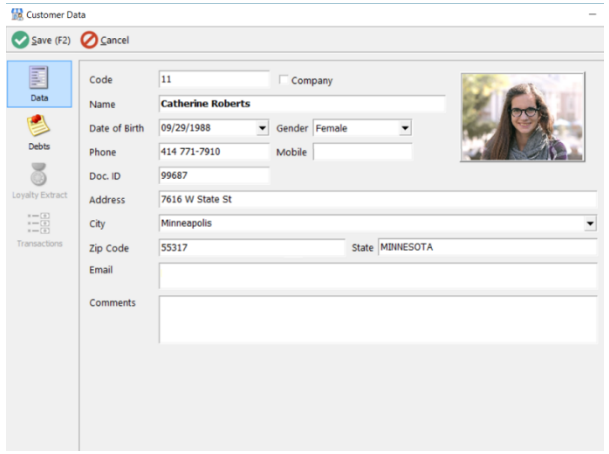
Sales Control



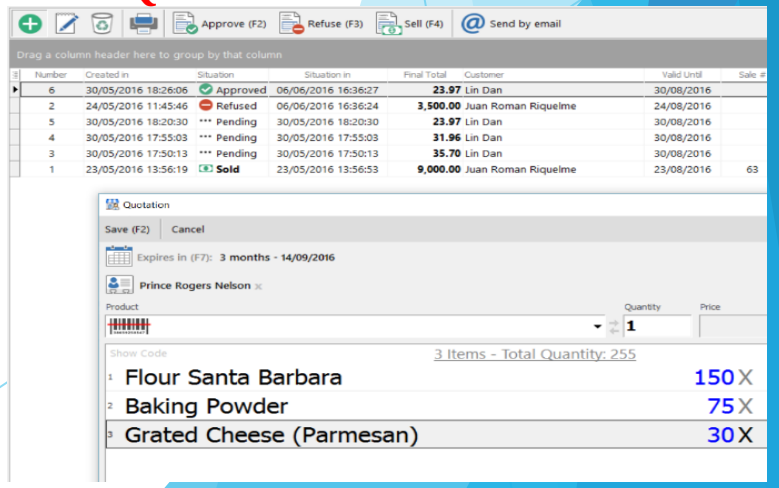
Cash Register Control



Customer Control



Quotations



ELECTRONIC SALES SUPPRESSION (ESS)

Electronic sales suppression (ESS) techniques facilitate **tax evasion** and result in **massive tax losses globally**.

Point of sales systems (POS) are expected to contain the original data which tax auditors can inspect.

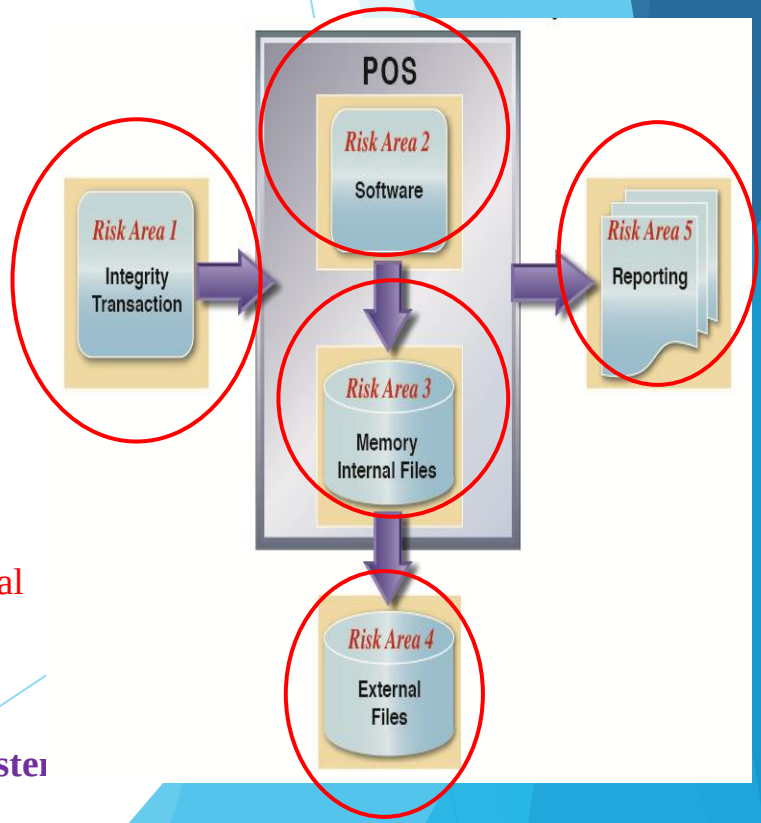
HOWEVER IN REALITY such systems not only permit **"skimming"** of cash receipts just as much as manual systems like a cash box, but once equipped with **electronic sales suppression software,** they facilitate far more elaborate frauds because of their ability to **reconstitute records to match the skimming activity.**

ECR/POS functions software abuse – programming options to facilitate for example :

- stop certain items, such as refunds, voids and other negative transactions, from appearing on the report or journal;
- stop certain items from being added to the grand totals;
- use the training mode - items are not recorded in the normal reports;
- reset grand totals and other counters to zero, or in some cases any specified number and
- specify that certain line items are programmed so that they do not appear in the report or journal.

The **program choices to select these items** are not hidden within the programming (unlike Phantomware)

Phantomware is a **software program already installed or embedded** in the **accounting application software** of the ECR or computerised POS system.
It is concealed from the unsuspecting user - accessed by clicking on an **invisible button** on the screen **or** a **specific command sequence** or key combination to bring up a Menu of options for selectively deleting sales transactions and/or **for printing sales reports with missing lines**.
When sales are deleted, the tool can automatically adjust inventory details **to avoid an apparent mismatch**



Zappers are **external software programs** for carrying out sales suppression - carried on some form of external electronic device like : USB keys, removable CDs, or they can be accessed on line through an internet link.
Zappers are designed, sold, and maintained by the same people who develop industry-specific POS systems.
They more difficult to detect because of their sophisticated design and because the offending software is not present on the machine **during normal use.** Brings up a **special screen on the POS syste** which allows the business owner to commence deletingand/or modifying sales.

BREAK AWAY SESSION - CASE STUDY

JOLLY RODGER WHOLESALERS

TAX AUDIT - CONSIDERATIONS : SUSPECT ESS WHAT NOW?

1. Determine the **software and version utilised** by taxpayer and if licenced (and how it is/was maintained)
2. Determine WHERE the raw data generated by POS is stored/kept
3. Obtain the data - either by request or seizure (consider if element of surprise is required) - **Chain of evidence**
4. Obtain understanding of **structure of reports** : which reports are generated
5. Obtain system description : number of users, how are they identified, when is transactions processed in stock
6. Understanding of **WHEN, HOW and by WHOM the sales and inventory transactions are actually processed in Accounting Records**
7. Obtain understanding of how : cash payments, card payments, gift cards and electronic **payments are accounted**
8. Look for : **quotation functionality, test user function, training function,** etc.
9. Identify the **super users** with access to data and processing
10. Some pointers on **"File Preparation" for tax audit analysis** :

There are differences in the various POS systems **but all POS systems have a relationship between the "Header Sales" file, the "Detail Sales"** file, and the "Tender" file. Typically the **total field in the Header file is equal** to the **summary or total of the payments in the tender file.**

9.1 **The "Header Sales" file** : Contains a single record for each sale or bill in the POS system. Some of the fields typically include a unique identifier (called a transaction ID), various data and time fields (order date/time, close of invoice data/time, etc.), invoice number, invoice amounts, **taxes,** transaction status codes, and employee identification.

9.2 **The "Detail Sales" file** : Contains multiple records or line items associated with each invoice **controlled by the unique identifier number**. The date and time of the order, items ordered, quantity, price, and amount are included. Other fields that the "Detail Sales" file may have are bill reference number (references that are printed out on the hardcopy bills) and item-ordered categories.

9.3 **The "Payment" file** : is the payment file and is populated by the payment or tender method used **by the customer to pay the bill**. Tender methods include : cash, various types of credit cards, debit cards, and gift cards. Also included are the unique transaction identifier number, payment date and time, tender type code, and payment amounts. Other fields that may be included are credit/debit card information, transaction status code, and employee identification.

TAX AUDIT – ANALYSIS : FILE PREPARTION

Preparing the *data files for analysis involves many steps that seem complex at times*. This is especially true when you are performing the steps for the **first time for POS systems** you might not have encountered before.

By understanding the **file-preparation steps** you consider to apply similar steps to other POS system data files.

- ✓ The **objective is to end up with a good master file** that you can use as the basis for your analysis.
- ✓ Your is aimed analysis to reconcile the **SALES DATA to the SALES REPORTS** generated by the POS system, and then to the **REPORTED SALES and VAT/GST in ACCOUNTING SYSTEM**
- ✓ and then lastly **BANK ACCOUNTS**

(To **exclude all transactions other than those that were closed or completed.** Typically, *"closed transactions"* are coded with the letter **"C"** in the STATUS field. Other status items, such as the letter "V" representing *"voids"*, should not be included as sales.)

There are a number of focus areas in analysis of the taxpayer's POS system and software, in main :

1. Determine if the POS system is **used exclusively** to account for sales – or is manual transactions outside the system allowed (recorded?)
2. What happens if power supply is **interrupted** (loadshedding, etc.)
3. Determine if **all terminals at all times are connected** to the POS system – what is the reason if not (how many is non-operational each day and what is the reason)
4. Is the version of the **POS software reliable** and updated regularly (or not) – by whom and when
5. Determine if the **POS system commands "fire" correctly** i.e. the system is consistent in processing transactions daily, weekly and monthly (missing days and hours)
6. Establish if there is a difference between reports : **Sales Report = Payment Report, or not (inclusive of negative sales, credit notes, customer rebates, voids) The percentage of sales in cash vs. other means (when?)**
7. Establish if there is a difference between **Stock Stats Item Report and Sales Report (number of items sold, pilferage/breakage and "adjustments" considered)**

TAX AUDIT – ANALYSIS : FILE PREPARTION

Step 1. **Isolate the "Header Sales" files** - This field identifies ALL sales but excludes discounts and taxes

Step 2. **Summarize the "Detail Sales" file** by the **unique transaction identifier of TXNID (transaction index)** and total the fields of PRICE, AMOUNT, and NETAMOUNT. Fields to include in the output file are ORDERTIME_DATE and ORDERTIME_TIME.

Step 3. Within the "Detail Sales" file, **highlight NO_OF_RECS** - This identifies that the number of records came from the "Detail Sales" file.

Step 4. **Join the "Header Sales" file to "Detail Summary."** Designate the "Header Sales" file as the primary file and the "Detail Summary" file as the secondary file. **Use TXNID as the Match Key Fields** and select the **"All records" in both files join option.** You now have all the fields and information from both files together.

Step 5. There might be duplicate records in this particular file (TXNIDs) in the **"Payment" file** due **to a payment and then a reduction due to discount, refund**, etc. in the PAYAMOUNT field. Perform a summarization by TNXNID and PAYMENTTYPEID, and total on the PAYAMOUNT and GRATUITY fields using the "Payment" file. Fields to include in the output file are the *Payment : description, date, time of payment fields*.

Step 6. Using the **"Payment Summary"** file, then **extract all noncash gratuities** when you perform various cash versus noncash types of analysis later.

Step 7. Perform a summarization on the **"Payment Summary**" file by using **Payment description as the field to summarize** and use the Numeric fields to total option on the fields NO_OF_RECS, PAYAMOUNT_SUM, and GRATUITY_SUM.
This provides us with a **total of the number of transactions, amounts paid, and gratuities for each payment type**

Step 8. Perform further analysis and comparisons to cash received vs. other payment methods. Compare **total Sales in the joint file with : Payment Summary report. Then compare to accounting records transactions for day, month and year**

Header Sales.IMD | Detail Sales.IMD | 1 Detail Summary.IMD

	TXNID	DETAIL_NO_OF_RECS	PRICE_SUM	AMOUNT_SUM	NETAMOUNT_SUM	ORDERTIME_DATE	ORDERTIME_TIME
1	1	6	18.6500	18.6500	18.6500	09/07/2007	01:00:13
2	3	10	52.3000	52.3000	52.3000	09/07/2007	15:01:25
3	6	7	44.8500	47.3500	47.3500	09/07/2007	15:12:13
4	7	4	24.2000	24.2000	24.2000	09/07/2007	15:13:42
5	8	6	27.5500	27.5500	27.5500	09/07/2007	15:18:32
6	9	1	9.9500	9.9500	9.9500	09/07/2007	15:22:01
7	10	3	19.1500	19.1500	19.1500	09/07/2007	15:45:29
8	11	3	14.8500	14.8500	14.8500	09/07/2007	15:55:20
9	13	3	11.1500	11.1500	11.1500	09/07/2007	15:59:17
10	14	3	16.8500	16.8500	16.8500	09/07/2007	16:04:54
11	15	1	8.9500	8.9500	8.9500	09/07/2007	16:11:02
12	16	6	25.9500	27.4500	27.4500	09/07/2007	16:19:01
13	20	2	55.9500	59.9500	59.9500	09/07/2007	16:57:15
14	21	3	24.1500	24.1500	24.1500	09/07/2007	16:58:45
15	22	3	0.00	0.00	0.00	18/07/2007	21:24:23
16	26	10	68.1000	68.1000	68.1000	19/07/2007	14:35:42
17	27	3	14.5000	14.5000	14.5000	19/07/2007	15:40:44
18	28	3	21.7500	21.7500	21.7500	19/07/2007	15:45:51
19	30	4	30.1500	30.1500	30.1500	19/07/2007	15:52:03
20	32	4	0.00	0.00	0.00	19/07/2007	15:59:49
21	33	1	1.1000	1.1000	1.1000	19/07/2007	16:01:13
22	34	1	7.7500	7.7500	7.7500	19/07/2007	16:02:20
23	35	1	7.7500	7.7500	7.7500	19/07/2007	16:03:09
24	36	1	5.2500	5.2500	5.2500	19/07/2007	16:04:56
25	37	4	8.2500	8.2500	8.2500	19/07/2007	16:05:29
26	38	3	3.3000	3.3000	3.3000	19/07/2007	16:05:38
27	39	2	21.7500	21.7500	21.7500	19/07/2007	16:07:34
28	41	8	38.2500	38.2500	38.2500	19/07/2007	16:12:12

Tender.IMD | 1 Tender Summary.IMD | 1 Non Cash Gratuity.IMD

	TXNID	TENDERTYPEID	NO_OF_RECS	PAYAMOUNT_SUM	NON_CASH_GRATUITY	TENDERDESC1	PAYTIME_DATE	PAYTIME_TIME
386	116000	4	1	10.5000	0.1600	Debit	02/04/2010	18:59:16
387	117985	4	1	10.0000	0.1100	Debit	20/04/2010	19:13:03
388	118094	2	1	25.0000	3.8600	MasterCard	21/04/2010	20:23:11
389	118308	4	1	30.0200	3.3000	Debit	23/04/2010	16:56:32
390	118333	4	1	11.0000	0.8800	Debit	23/04/2010	18:05:14
391	118335	2	1	9.0000	0.0100	MasterCard	23/04/2010	18:26:46
392	118377	2	1	3.0000	0.6800	MasterCard	23/04/2010	19:48:11
393	118694	2	1	5.0000	1.2200	MasterCard	26/04/2010	19:21:59
394	118948	2	1	6.2500	0.0300	MasterCard	29/04/2010	12:28:27
395	119002	2	1	50.0000	7.1700	MasterCard	29/04/2010	19:16:00
396	119179	2	1	20.0000	5.3100	MasterCard	30/04/2010	21:04:07
397	119237	4	1	10.0000	1.2400	Debit	01/05/2010	16:51:47
398	119354	2	1	40.0000	7.0600	MasterCard	02/05/2010	16:23:01
399	120059	2	1	22.0400	0.6200	MasterCard	08/05/2010	17:40:15
400	120086	2	1	25.0000	3.5800	MasterCard	08/05/2010	18:18:13
401	120519	4	1	21.0000	2.3500	Debit	11/05/2010	19:11:27
402	120727	4	1	10.2000	2.0100	Debit	13/05/2010	18:22:28
403	120869	5	1	10.0600	1.3000	AME	14/05/2010	19:14:48
404	121415	2	1	20.0000	2.1500	MasterCard	19/05/2010	19:21:24
405	121501	4	1	10.2500	0.1300	Debit	20/05/2010	18:35:53
406	121733	2	1	65.0000	2.8500	MasterCard	22/05/2010	16:59:19
407	121805	2	1	6.7000	0.0300	MasterCard	22/05/2010	20:52:05
408	122534	2	1	25.0000	3.3000	MasterCard	29/05/2010	20:21:38
409	122820	4	1	40.0000	13.2100	Debit	01/06/2010	17:22:20
410	122827	4	1	30.0000	4.9700	Debit	01/06/2010	17:44:49
411	123048	2	1	20.2600	0.1500	MasterCard	03/06/2010	16:36:38

1 Tender Summary.IMD | 1 Tender Types.IMD

	TENDERDESC1	NO_OF_RECS1	NO_OF_RECS_SUM	PAYAMOUNT_SUM_SUM	GRATUITY_SUM_SUM
1	AME	735	735	13,655.7500	1.3000
2	Cash	20524	32092	288,592.7600	0.00
3	Debit	52519	52540	1,006,967.4600	139.9500
4	Gift Certificate	43	44	852.9800	0.00
5	MasterCard	5318	5319	140,576.5600	2,008.2800
6	No Change	4	4	-37.6200	0.00
7	Visa	6712	6712	199,755.9600	0.1100

LEGISLATION AND POLICIES – CASH REGISTERS, ESS : VAT EVASION/REFUNDS

Electronic Sales Suppression: A threat to tax revenues - Published 18 February 2013

This report describes the functions of point of sales systems and the specific areas of risk to tax administrations. It sets out in detail the electronic sales suppression techniques that have been uncovered, in particular "Phantomware" and "Zappers", and shows how such ***methods can be detected*** *by tax auditors and investigators.*

The report also considers a ***number of strategies*** *adopted in different countries to* ***tackle electronic sales suppression and highlights best practices****. In particular, it makes a number of recommendations to countries for addressing this important area of risk.*

Different approaches

Ultimate Goal : Electronic cash registers that deliver **real-time sales data to tax administrations**, or data sharing that **produces pre-filled tax returns**

- **Electronic invoices only: Egypt** – From November 2020 is obliging of **500 largest taxpayers** to sign up for a program to submit their invoices electronically
- **Mandatory invoicing and cash register monitoring: Québec** mandated and subsidized the deployment of **40,000 "sales recording modules," tamper-proof microcomputers** attached to every electronic cash register. Each SRM has the capacity to store sales records in a secure memory, generate invoices bearing a unique digital signature, and produce summary reports for inspection by Revenue Québec.
- **Cash registers has to be registered and certificated by tax authority before being admitted to the market :**

- **Poland** - both structural solutions and software in a fiscal registers are examined by the public authority - Central Repository of Cash Registers (CRK) entered into force **on May 1, 2019**. Until the 22 November 2021 **704,000** online cash registers, including 4000 virtual cash registers, have already been registered.
- **Philippines -** requirement for the inspection, evaluation and registration of Cash Register Machines (CRMs) and Point-of-Sale Machines (POSs) prior to their use**, "Permits to Use"**.
- **Sweden, Romania, Russia** - Companies are required to use a certified cash register and provide customers with receipts. The cash register must be registered with the supervising authority (e.g. tax administration) and comply with detailed specifications. The tax administration may perform inspections as well as disguised visits to verify that transactions are registered and receipts are provided to customers.

LEGISLATION AND POLICIES – CASH REGISTERS, ESS : VAT EVASION/REFUNDS

➢ **Cash registers has to be registered and certificated by tax authority before being admitted to the market :**

- **Norwegian Cash Register Systems Act** - from 1 January 2017 all cash register systems have been required to comply with the and associated Cash Register Systems Regulations.
- **France -** By virtue of Article 88 of the 2016 Finance Law No. 2015-1785 dated December 29th 2015, cash register system owners must, beginning on January 1st 2018, use cash register systems meeting the conditions of data inalterability, security, conservation and archival in preparation of tax authority control.

➢ **Fiscalization of cash registers is mandatory -** Certain countries in **Europe.**

- Protection of the cash register's **transaction logs against manipulation**. A principle similar to that of the blockchain is used for this purpose. **Cash register receipts are chained together. Each cash register transaction is identified by a signature**. Manipulation causes an interruption of the signature chain. This means that it can be immediately identified by an audit by the tax office.
- **Germany** - since 01 January 2020,The receipt must be printed out as an “annual receipt”, checked by using the “BMF Belegcheck”- App and kept for **seven years**.
- **Hungarian** Government implemented The Online Cash Register System (OPG) legislation in 2014, starting with retail and hospitality sectors and in 2016 extending it to the service sector. In total **250 000 cash registers** are connected to the Tax Authority’s central data analysis system.
- On 01.04.2017, the **Austrian** Cash Register Security Regulation (RKSV) entered into force. Each cash register must be equipped with a technical security device for protection against manipulation. A feature of the RKSV is an additional, machine-readable code (QR code) on the document.

➢ **Penalties**

- **Australia (ATO)** - Ban on electronic sales suppression tools - This includes assisting an individual or business to possess or use an ESST, such as a software developer, supplier, maintenance technician or tax professional, we encourage you to do the right thing and let us know.

➢ **Voluntary Disclosure**

- HMRC Voluntary Disclosure registration by 5 January 2023 and the disclosure must be completed by 28 February 2023.

➢ **Some jurisdictions have also criminalized the provision, possession or use of electronic sales suppression software.**

THE JOINT CHIEFS OF GLOBAL TAX ENFORCEMENT (KNOWN AS THE J5) – 9 DECEMBER 2022 STATEMENT

J5 launches international probe into sales suppression software

▶ NEW YORK – The Joint Chiefs of Global Tax Enforcement (J5) launched an international probe into the use of sales suppression software. The probe resulted in the arrest of five individuals in the United Kingdom who allegedly designed and sold electronic sales suppression systems internationally.

▶"This was a **highly sophisticated, truly global attack on the international tax system**," said Simon York, Director of His Majesty's Revenue & Custom's (HMRC) Fraud Investigation Service. "The group behind this activity is suspected of **enabling thousands of businesses to evade tax in what is a large-scale, technologically enabled fraud**.

▶**Our ground-breaking response, with internationally co-ordinated action**, marks a significant moment in our efforts to close the net on those we suspect of designing, supplying and using electronic sales suppression software. Most businesses pay the tax that they owe. HMRC is on the side of this honest majority and our action helps to ensure they are not being under-cut by tax-evading competitors. This is just the beginning of our work in this area, and we already have other suspected suppliers in our sights. We are urging all users of these types of systems to come to us before we come to them."

▶Electronic sales suppression software permits businesses to hide sales on their electronic point of sales system to evade paying taxes on incurred sales. The software manipulates records by **deleting sales and routing credit card payments through an offshore bank. The system was allegedly first introduced in the United Kingdom and then exported to businesses in the United States and Australia** during the COVID-19 pandemic.

▶In addition to the United Kingdom, the **J5 conducted coordinated actions in the United States and Australia** to target software suppliers and users as part of the probe.

▶"Adding ESST [electronic sales system technology] to your point-of-sale system is a deliberate and underhanded act designed purely to under-report income and avoid tax obligations," said John Ford, Deputy Commissioner of Integrated Compliance at the Australian Taxation Office. "**It's illegal, and it will not be tolerated here in Australia**. Businesses using or promoting this technology are effectively stealing from the Australian community, and that's simply not ok. Through the international collaboration (with J5), we have access to a global network of intelligence analysts and investigators – it's only a matter of time before you're caught by us, or one of our partners."

OECD GUIDANCE ON ELECTRONIC SALES SUPPRESSION

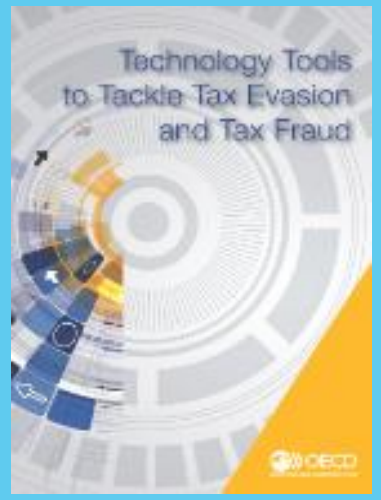
Electronic Sales Suppression: A threat to tax revenues

Published on 18 February 2013

Download the report (PDF):

- English
- French
- German
- Russian
- Spanish

This report describes the functions of point of sales systems and the specific areas of risk to tax administrations. It sets out in detail the electronic sales suppression techniques that have been uncovered, in particular **"Phantomware" and "Zappers"**, and **shows how such methods can be detected by tax auditors and investigators**. The report also considers a **number of strategies** adopted in different countries to tackle electronic sales suppression and highlights best practices. In particular, it makes a number of recommendations to countries for addressing this important area of risk.



Technology Tools to Tackle Tax Evasion and Tax Fraud

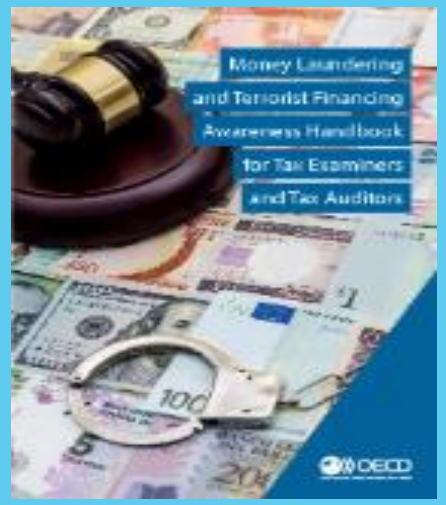
Published on 31 March 2017

Download the report (PDF):

- English
- German

This report provides an overview of some of the **technology tools** that tax authorities have **implemented** to address tax evasion and tax fraud, **focusing on electronic sales suppression and false invoicing**. The report also includes a more **technical catalogue of these technology solutions**, with a view to encouraging other tax authorities that are facing the same types of risks to draw on that experience. The report also discusses complementary work that tax authorities are undertaking to address the cash economy and sharing economy, which, although not types of tax evasion and fraud themselves, can facilitate it.

OECD GUIDANCE TO FINANCIAL CRIMES AND MONEY-LAUNDERING



Money Laundering and Terrorist Financing Indicators: a handbook for tax auditors and tax examiners

Published on 13 June 2019

Download the report (PDF):

- **English**
- **French**
- **German**
- **Russian**
- **Dutch**
- **Spanish**
- **Korean**
- **Portuguese**

First launched in 2009 as a practical tool to assist tax authorities in identifying money laundering during the course of normal tax audits, this revised handbook includes updated money laundering indicators and new material to increase detection and reporting of terrorist financing.

The OECD's Global Relations Programme announced the **launch of a new on-line course focused on Money Laundering and Terrorist Financing Indicators**: a handbook for tax auditors and tax examiners.

About this course:

This e-learning module provides specific money laundering and terrorist financing indicators that will help auditors and examiners **identify these activities during the course of their normal tax audits.**

The course, which includes a **great number of case studies**, describes the nature of money laundering and terrorist financing activities, **emphasizes the roles of auditors and examiners in countering** these practices, **and describes practical resources and tools that are available for effective detection and deterrence**.

This Handbook should complement but not replace domestic policies and procedures. To that end, it is designed so that tax administrations can adapt it to suit their domestic context, taking into account the varying roles that tax administrations have in relation to reporting unusual or suspicious transactions, receiving suspicious transaction reports and investigating money laundering offences.