WHAT'S INSIDE?

- Elderly Warned Against New Bank Scam
- Covid-19 fuelling rise in human trafficking, UN warns
- Ferlio Notification Board
  - Birthdays
  - Motivation
  - Charity
- Specialist Services Offered / Contact Us
- Investigator of The Month: Japie van Niekerk – Retail Fraud
- Ida Mostert – Occupational Therapists
- IAFCI 2nd Annual Virtual Conference – A practical Guide to Forensic and Fraud Investigation

Ferlio

Group of Investigators

0860 337 546 / 0860 (F-E-R-L-I-O)

NEWSLETTER

Volume 05 – April 2021

We enter into the fourth month of 2021 and we begin to see the weather cooling down as summer comes to an end and autumn travels towards us. Soon enough the trees will lose its leaves and the mornings will become cold. Unlike the seasons, one cannot always accurately predict the plans a fraudster or criminal has in store for us. New criminals arise daily, and businesses as well as individuals need to keep their eyes open at all times.

In this newsletter, you will find an article about a new bank scam which targets the elderly, how Covid-19 is connected to the rise of human trafficking and the investigator of the month discusses Retail fraud.

ELDERLY WARNED AGAINST NEW BANK SCAM

BY SHANICE NAIDOO

https://www.iol.co.za/weekend-argus/news/elderly-warned-against-new-bank-scam-019e9d31-932a-47f5-9435-df0d2e2a86bf

Cape Town - The elderly are being targeted in the latest bank fraud scam.

"Several cases reported since January this year. The value involved is over R700 000. In a few cases, the bank was able to freeze the account so that the funds didn't get released. The victims are elderly persons," said Port Alfred police spokesperson Captain Mali Govender.

National police spokesperson Brigadier Vish Naidoo said while he was not aware of reports in other areas, people from different provinces are not immune to the scam.

The SAPS issued a warning stating that fraud cases are a crime of concern as criminals are using another trend to defraud persons.

The caller will identify himself as an individual working in the bank's fraud division. He/she states that a transaction has taken place on the victim's account. The suspect has all personal particulars and profile of the victim, including details of bank accounts, linked accounts and beneficiaries.

"The suspect then states that a transaction has appeared on an account which appears suspicious and enquires from the victim if they have approved a transaction for a large amount of cash from their account, furnishing account

details and when the victim replies in the negative, the caller informs the victim that he will reverse the charge if the victim can go onto their banking app," read the statement.

Once the victim has logged onto their banking app, the suspect tells the victim to supply the one-time password (OTP) that was sent via SMS to their cell phone so that the transaction can be reversed. As soon as the OTP is given to the suspect, the suspect starts to transact on the account, increasing limits, adding beneficiaries and making payments.

Head of fraud strategy at Absa retail and business bank Ulrich Janse van Rensburg said over the past 18 months, they had noted an increase in social engineering, where fraudsters or syndicates trick customers into disclosing their personal and confidential information. With social engineering syndicates typically pretend to be from a bank and share personal information often causing customers to let their guard down and disclose confidential information.

"As an industry, we are alive to the threat that this modus operandi poses to customers and we are working closely with other banks, and the SA Banking Risk Information Centre in combating this," said Van Rensburg.

The South African Banking Risk Information Centre (Sabric) told the Weekend Argus that they are aware of this modus operandi.

Chief executive of Sabric Nischal Mewalall said bank clients have lost money in this way due to social engineering tactics, as these incidents are reported by the victims to the banks. This modus operandi sees criminals utilise social engineering tactics which are designed to manipulate victims into disclosing their confidential information such as PINS and passwords to access their bank account.

When asked about stats, Sabric said their latest digital crime stats will be released in June.

"Sabric has been very vocal about awareness messaging around vishing, smishing and phishing, all specifically highlighted due to the proliferation of these tactics. The banks also deploy campaigns and awareness messaging to educate their clients and constantly re-engineer their processes because of their engagement with consumers around these fraud tactics," said Mewalall.

Standard Bank's spokesperson, Ross Linstrom, said they take the protection of their customers' personal and banking data very seriously.

"We encourage all customers to be always vigilant and to not volunteer any private information via email or telephonically. It's important to stay up to date with the latest scam trends so you can protect yourself. Never share your one-time pin with anyone (including the bank)," said Linstrom.

He added that this scam is known as vishing. Vishing is when scammers pretend to be somebody from the bank and acquire your private information through telephonic manipulation.

"Be conscious of the fact that criminals can mask their telephone numbers seem as if a legitimate individual or company is making the phone call," said Linstrom.

He added that If you receive an OTP on your phone without having transacted yourself, it is likely that it is a fraudster who has used your personal information. Do not provide the OTP telephonically to anybody.

COVID-19 FUELLING RISE IN HUMAN TRAFFICKING, UN WARNS

BY THE EASTAFRICAN

https://www.theeastafrican.co.ke/tea/news/east-africa/rise-in-human-trafficking-3278602

A new report by the UN drug and crimes agency warns that the Covid-19 pandemic could also be contributing to a rise in trafficking of persons.

The Trafficking in Persons Report released on Tuesday says poverty arising from lost jobs or other economic opportunities has, over the last one year, increased the pool of people most vulnerable to being trafficked.

"Millions of women, children and men worldwide are out of work, out of school and without social support in the continuing Covid-19 crisis, leaving them at greater risk of human trafficking.

"We need targeted action to stop criminal traffickers from taking advantage of the pandemic to exploit the vulnerable," said UNODC Executive Director Ghada Waly on Tuesday.

The warnings came even as the same document suggests countries, especially in the Sub-Saharan Africa region, had their agencies working hard, detecting trafficking incidents mostly before the victims crossed borders.

According to an analysis in the 2020 Trafficking in Persons Report by the UN Office on Drugs and Crime (UNODC), an assessment of sub-Saharan African countries including Kenya, Uganda and Ethiopia showed that there had been fewer incidents of domestic trafficking. But 75 per cent of incidents detected involved victims destined to neighbouring countries, even though the police, immigration and other security agencies often foiled them on home soil.

Children, trafficked for sexual exploitation, forced labour and begging, constituted 30 per cent of all incidents observed in sub-Saharan Africa. This was also the time most countries on the continent shut down schools to control the pandemic.

In East Africa, seven in every 10 traffickers arrested were male and most of them were arrested on home soil as they plotted to export the victims.

This data could indicate that regional agencies were working hard to curb trafficking.

However, the data also shows the number of children trafficked more than doubled to 30 percent in two years. Globally, data on women trafficking victims fell to 50 percent from 70 in 2018, but in sub-Sahara Africa, women and children constituted 86 per cent of trafficked victims. Ethiopia has more than half of it children involved in child labour, alongside Chad, Benin, Niger, Mali, Cameroon and Sierra Leone.

Researchers at the UN agency based in Vienna, Austria, say they assessed trends over the last one year globally and found that traffickers target the marginalised or people in difficult circumstances such as being in urgent need of employment or having invalid immigration papers. These conditions, the report says, are likely to worsen as the pandemic continues.

The data emerged from an assessment of 233 court cases involving human trafficking. And victims, most of who had either been rescued or detected travelling to their destinations, indicated they had been forced into the horrid trafficking to meet their basic needs.

"The Covid-19 pandemic will further amplify socio-economic inequalities, increasing the pool of potential victims," says the biennial document published on Tuesday.

The pandemic has not just curtailed people's access to economic opportunities. The UN says prosecution of those involved has had to be delayed, effectively denying victims their justice.

"The Covid-19 pandemic may have a negative impact on the provision of timely and fair legal proceedings, contribute to case backlogs and limit the legal services provided to victims of trafficking."

Though the report does not give specific anecdotes on Kenya, the country is among the several in sub-Saharan Africa analysed.

Kenya's Counter-Trafficking in Persons Act enhanced the penalty for sex trafficking and forced labour and offenders risk life imprisonment or Ksh30 million (approximately $300,000) if found guilty.

But Covid-19 delays which have in the recent past forced courts to shut down or cases to be postponed could continue in future if the pandemic persists.

"Countering trafficking effectively also requires tackling related forms of transnational organised crime, as well as cybercrime and corruption," said Ghada Waly, Executive Directive of UNODC.

"As the Trafficking in Persons Protocol highlights, to prevent trafficking governments need to address poverty, underdevelopment and a lack of equal

opportunity, and raise awareness. An inclusive recovery must create opportunities and give hope to young people and the disadvantaged."

The UN agency's report concurs with a similar, annual one, produced by the US State Department. Last year, it said "scarce economic opportunities and dire poverty, coupled with familial encouragement" had compelled many East Africans to leave their homes.

It cited illegal border crossings into Kenya by Ethiopians seeking greener pastures in South Africa.

FERLIO NOTIFICATION BOARD

BIRTHDAYS

We here at Ferlio wish you have a wonderful birthday and a prosperous year ahead.

- Leon Mans – 15 April 2021
- Theo Weyers – 16 April 2021
- Ben Lindeque – 18 Apr 2021
- Dion Pienaar – 23 April 2021
- De Wet Ferreira – 30 April 2021
- Kevin van Zyl – 01 May 2021
- Steven Botha – 03 May 2021
- Jurie Human – 05 May 2021
- Kevin Smith – 09 May 2021
- Johan Goosen – 16 May 2021

MOTIVATION FOR THE MONTH:

CHARITY OF THE MONTH

THE PINK LADIES ORGANISATION FOR MISSING CHILDREN

The Pink Ladies are an independent group of volunteers, affiliated and associated with The Pink Ladies (a registered Section 21 NGO). The organisation was established for the primary purpose of reuniting missing and endangered children and loved ones with their families and/or caregivers. The group does not charge for its services which are provided by The Pink Ladies strictly voluntarily and performed for the love of children everywhere in South Africa regardless of colour, creed or circumstance.

Not all cases of missing and/or exploited children make headlines, and a large percentage are never reported to the police or social workers.

We assist by taking an interest and assisting where possible. We act within strict protocols and operate within the laws of our country. We do not act in a vigilante manner, nor do we condone such behaviour. Among our members and volunteers are lawyers, psychologists, pastors, private investigators and criminologists as well as ordinary members of society, all of whom lend their professional skills to assist in the recovery and return of missing, exploited and runaway teenagers and spouses. This is done in a variety of ways including raising awareness, assisting with the reporting of missing children and adults and referring to specialist guidance as and when required.

The South African Police Service is almost always involved, and we have a fine professional relationship with them. We are independent volunteers driven by passion and our love for children.

The Pink Ladies is an NGO (Section 21) Company, duly registered in accordance with the Company Laws of the Republic of South Africa under Reg. No. 2007/018067/08

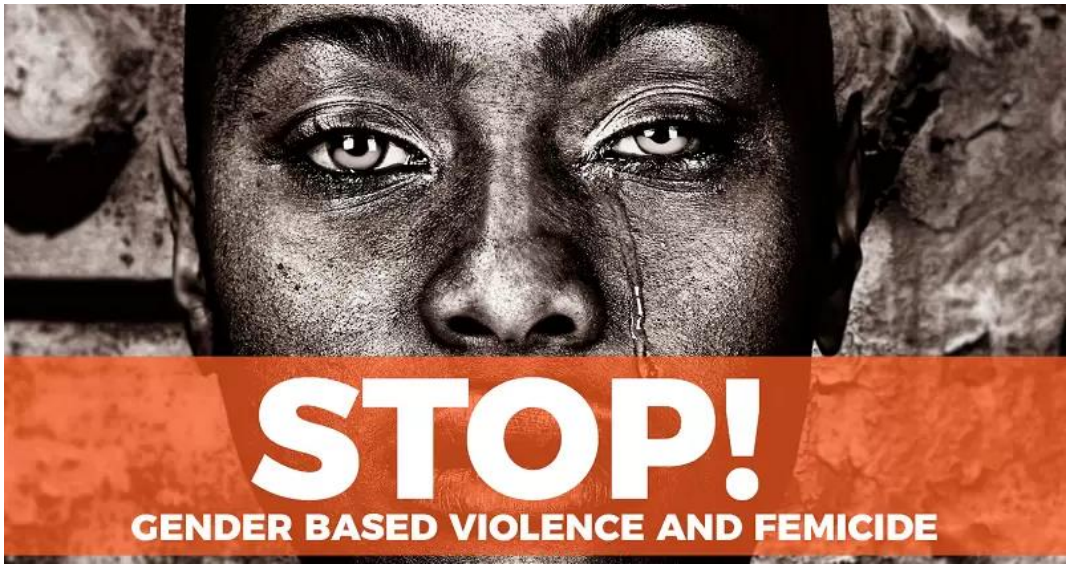
Banking Details:

Standard Bank of SA Ltd

Acc No. 271 624 256

Constantia Branch

Code 025309



Ferlio

Group of Investigators

SPECIALIST SERVICES OFFERED:

Investigations, including but not limited to:
- Criminal
- Civil
- Forensic
- Cyber

Profiling
- Profiling / Lifestyle audit of individuals
- Business profiling
- Strategic audits on business
- Fingerprint screening
- Financial Audit Investigations
- Employee Background Screening
  - Identification documents
  - Driver's License & PDP
  - Criminal record
  - Educational background & qualifications
  - Prior employment records
  - Credit status
  - Integrity testing
  - Identification photos
  - Fingerprint verification

Undercover agents
- Standard level agents
- High level agents
  - Strategic level agents

Surveillance
- Physical
- Static
- Electronic
- Counter
- Covert escorting

Close Protection
- Executive protection
- Executive Support
- Asset in transit protection

Handwriting Specialist & Fingerprint Specialist

Polygraphs

Fraud Detection Initiatives

Security Risk Assessments

Transcripts / Translations

Pre-employment Psychometric Assessments

Truck & Driver Inspections

Security Vulnerability Assessment

GET IN TOUCH:

Phone: 0860 337 546 / 0860 (F-E-R-L-I-O)

Email: office@ferlio.co.za

Find us on Facebook: @FerlioGroupOfInvestigators

Ferlio Group of Investigators
@FerlioGroupOfInvestigators · Private Investigator

INVESTIGATOR OF THE MONTH:

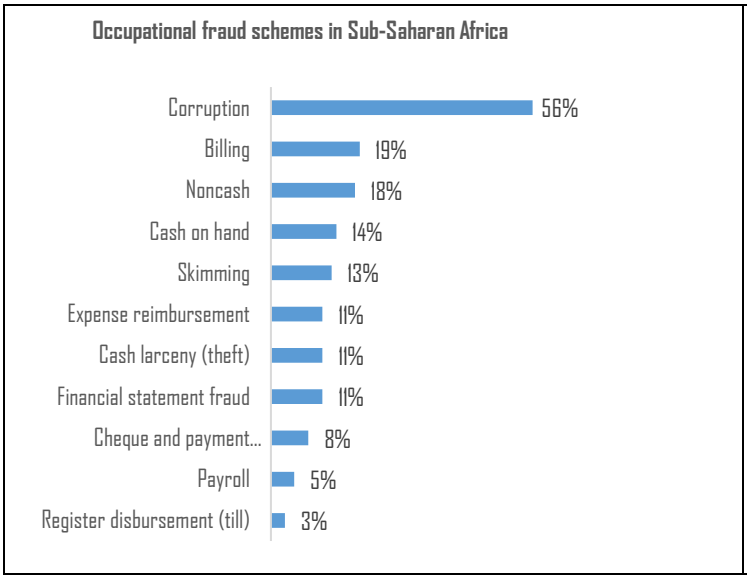
Japie van Niekerk

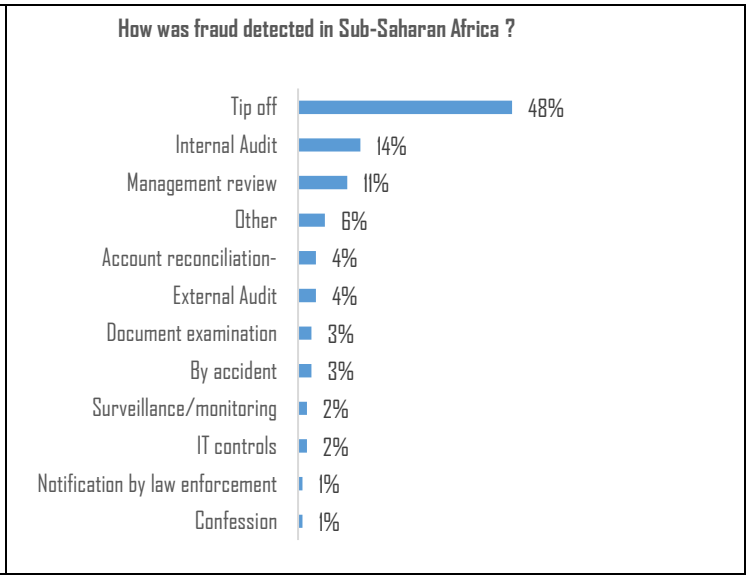
Retail Fraud

COVID-19 and the national shutdown in South Africa have placed businesses under great pressure. With the ever increasing unemployment rate, unscrupulous employees are looking at innovative ways to supplement their earnings.

As per the latest Report to the Nation – 2020 from the Association of Certified Fraud Examiners (ACFE), out of 2 504 cases reported on from 125 countries, Sub-Saharan African countries accounted for 301 cases (15%). South Africa accounted for 77 (25,6%) cases out of the 301 cases, the highest contributor in the Sub-Saharan Africa group. Kenya was second in the group with 53 cases and third was Nigeria with 49 cases.

The stats below were taken from the Report to the Nation – 2020 from the Association of Certified Fraud Examiners (ACFE).





The examples below illustrate the types of retail fraud perpetrated.

1. Loyalty program fraud - Customers are rewarded and encouraged to join loyalty programs offered by retailers. Loyalty cards are offered to customers who subsequently earn loyalty points each time a purchase is made. Examples of loyalty program fraud committed by unscrupulous cashiers are as follows;
   1) Cashiers pretend to enrol "new customers" to the loyalty program but instead link the card to themselves. The same card is then used when various purchases are rung up by the cashier throughout the day. Loyalty points are accumulated and the cashier redeems the points at the end of the day or when s/he has enough points to purchase for example airtime etc.
   2) Cashiers are given daily targets to offer and sign up customers to join the retailer's loyalty program. To reach their target, the cashier will fraudulently link loyalty cards to fictitious customers and then target cash-paying customers by using the loyalty cards when processing their transactions.

2. False credits – When a customer returns items s/he purchased from a retailer, a credit is processed by the cashier and the customer is refunded the amount s/he paid. A potential fraudulent activity committed by an unscrupulous cashier would be to add extra items onto the credit transaction when s/he processes it and to pocket the extra cash.

3. Gift card fraud – An unscrupulous cashier purchases the retailer's gift card on an unsuspecting customer's retail account. Thereafter, the cashier targets cash-paying customers by using the gift card (previously purchased on a customer's account) as tender type instead of tendering the customer's cash. This "swap" is done to balance his/her banking/cash-up at the end their shift and the cash is pocketed by the cashier.

4. Third party ticket sales – A customer purchases a ticket from a retailer to a social event, for example, a soccer match or concert. The cashier processes the ticket on the third parties' terminal and the ticket is issued to the customer. If the third parties' terminal is not integrated with the specific retailer's system, a separate transaction has to be processed on the retailer's terminal. Fraud can be committed when the unscrupulous cashier does not process the transaction on the retailer's system and pockets the cash.

5. Remote transactions – Each retailer has a Helpdesk that is responsible for resolving errors that occur during day to day operations at cashier's terminals in store. The Helpdesk operators have online access to in-store cashiers' terminals to resolve any errors. Fraud is committed when the dishonest Helpdesk operator processes a payment/credit transaction remotely on their own retail account when the cashier's terminal is unattended or not suspended.

6. Multiple gift cards processed – When a customer purchases a gift card at a retailer, the transaction is processed at the terminal by the cashier, who will swipe the gift card through the EFT (electronic fund transfer) device to activate the gift card. Fraud is committed when additional gift cards are swiped through the EFT device during the same transaction.

7. Fraudulent credit cards – Through collusion, dishonest cashiers and fraudsters use cloned credit cards to pay for high priced goods at retailers, e.g. cell phones, branded merchandise etc. The credit card is not inserted into the EFT device, but swiped through the device. If settings on the device are not set to reject swiped transactions, the transaction will be approved on the EFT device. Furthermore, no pin code is required on a cloned credit card.

8. Petrol claims – Dishonest employees who receive a petrol allowance for using their own vehicles for business purposes submit reduced private mileage thereby inflating their business mileage resulting in their reimbursement being inflated.

9. False sale slips and multiple credits – Cartons of clothing are stolen while in transit to either the warehouse or store. Usually these cartons contain the same style of garments with only a few size curves. The fraudster will make a genuine purchase at the retailer of only 2 to 3 items of the same product found in the cartons. A sale slip is obtained by the fraudster with the cash purchase. The fraudster now has a genuine slip which can be verified via the retailer's records. Blank journal rolls are purchased from dishonest employees at the retailer and the sale slip is photocopied onto the retailer's journal roll. Multiple copies are made and used to return all the goods in the cartons. Various stores are visited by the fraudsters so as to not draw attention. In this way, the fraudster is able to exchange the stolen goods for cash.

10. Cloned retailer card – Fraudsters collude with corrupt employee's employed at the Retailer to obtain customer information e.g. ID number, contact and work details etc. in order to clone the customer's retail card. The account card number/information is also shared with the fraudsters. The card detail is used to manufacture a cloned card. The customer's account details are studied so that all questions are answered correctly by the fraudster during the customer authentication process at the store.

11. Minibus taxi ordered at inflated prices – Employees who work late shifts (after 6pm) are transported to their place of residence. Minibus taxis are used to transport these employees when their shift ends. Unscrupulous store management and taxi owners collude to inflate the cost of transporting the employees. The number of taxis used is inflated when payment is made to the taxi owner.

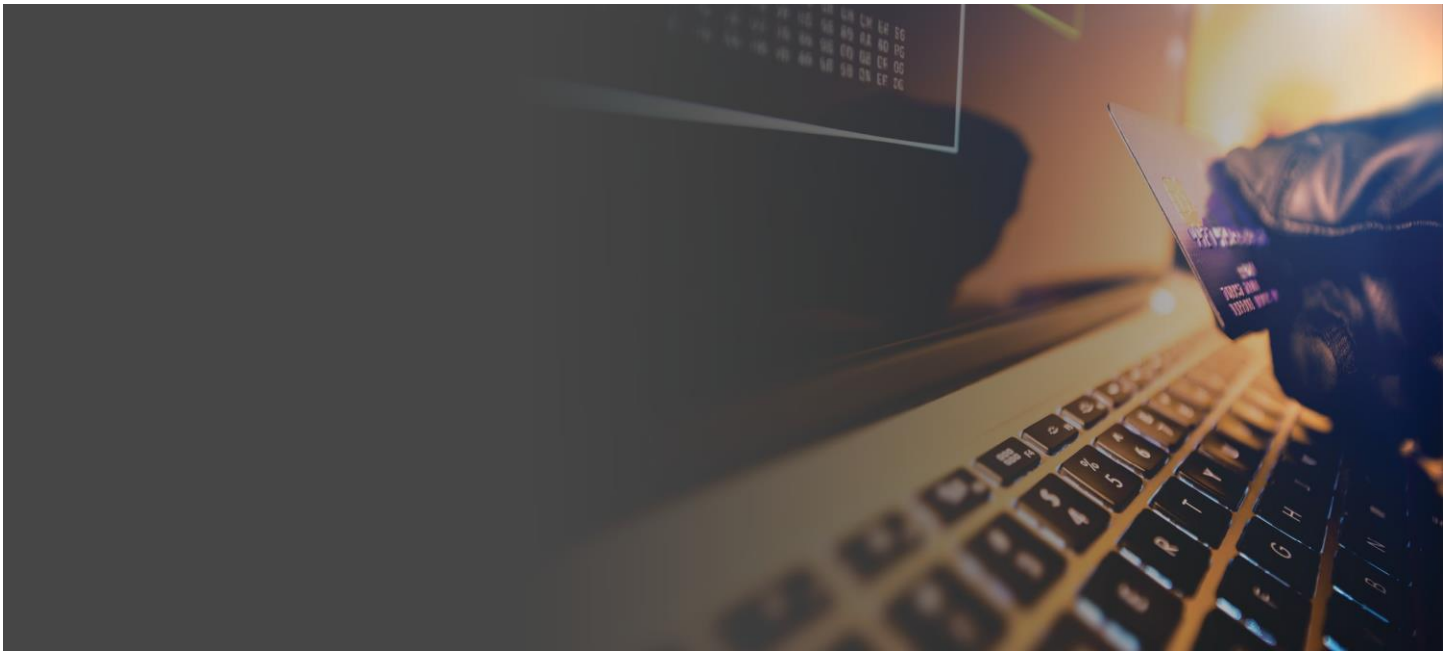
12. Fraudulent on-line purchases – Fraudsters illegally obtain a customer's account details. They then change the account details via the retailer's Customer Service department to the fraudster's details. On-line purchases are made on the customer's account and a one-time verification code is sent to the fraudster who uses it to validate the purchase. In this way the genuine customer does not know that purchases were made on their account.

13. Gift card purchase – A gift card is purchased at a retailer and a sales slip with pin code is given to the customer. Once the customer leaves, the dishonest cashier will reprint the transaction and send the pin code via a WhatsApp/SMS to the fraudster or corrupt a colleague. The fraudster/colleague will transfer the value of the gift card to another gift card and sell that gift card onto a willing buyer at a discounted price.

14. Employee staff discount – Majority of retailers offer employees a staff discount when they purchase goods from the retailer. Dishonest cashiers will target cash paying customers and process their purchases using the employee's staff account privileges. Unknown to the customer, the discount amount is pocketed by the cashier, as the customer pays the full price for the goods.

15. Cashier authorises price discounts – Some cashiers know/share each other's authorising passwords or certain members of management share their passwords with the cashiers in order to save time or minimal management members are scheduled to work, like Sundays/public holidays. A dishonest cashier will authorise discounts to relatives/fraudsters for self-enrichment by using someone else's authorising password.

Japie van Niekerk (CFE)
JVN PRIVATE FRAUD INVESTIGATIONS
Reg no: 2021/433496/07
Cellphone Number: +27(0) 82 706 5584
Email: Jvniekerk2@gmail.com



Ida Mostert Occupational Therapists

Services:

Ida Mostert Occupational Therapists is an innovative practice offering medico-legal services for various clients. Our assessments are done with the utmost professionalism, whilst our medico-legal reports are of high quality and submitted timeously.

We make use of the functional assessment tool, ErgoScience FCE, which enable us to make conclusions and recommendations based on scientifically approved assessment methods. ErgoScience testing protocols were developed at the University of Alabama at Birmingham and the research validating them has been published in peer-reviewed occupational medicine journals.

Using standardized tasks, verbal instructions and a proprietary scoring system with proven reliability and validity, the ErgoScience FCE can defensibly predict the ability to meet the demands of an 8-hour day. Each task has been individually validated so that job-specific testing can be performed.

Medico-legal services offered includes road accident fund claims, slip and fall accidents, work related injuries, medical negligence claims and functional capacity evaluations.

Vision Statement:

Ida Mostert Occupational Therapists is a medico-legal practice consisting of qualified, highly professional, and passionate therapists. We make use of our experience and knowledge gained over the past 10 years to provide out clients with innovative solutions ensuring implementation of best practices. Our vision is to create a working environment conducive of professionalism, honesty, integrity and open communication.

Mission Statement:

- We strive to establish ourselves as leaders in the medico-legal field, ensuring our clients receive professional services,
- We endeavour to offer high quality services in a timeous manner, based on scientifically approved assessment methods,
- We do not compromise on the quality of our reports, we strive to make use of the most recent and up to date assessment tools, enabling us to shorten turnaround time of our reports,
- We strive to ensure a professional working environment with emphasis on integrity and work ethics.

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

2nd Annual Virtual Conference – A practical Guide to Forensic and Fraud Investigation

The International Association of Financial Crime Investigators (IAFCI) is a non-profit organisation committed to fight white collar crime in the financial sector and has members across the Globe.

The Gauteng Chapter will be hosting our virtual conference on 21 & 22 April 2021, which is to be broadcasted from the Iris Room at Emperors Palace, next to OR Tambo International Airport.

The 2nd Annual Conference theme is "Practical solutions for forensic and fraud investigations", and our focus is to provide the delegates with practical presentations and/or case studies that will empower the delegates to implement the training provided at the conference.

The IAFCI conference is less than two weeks away! Register now for some of the PRACTICAL topics and earn 10 CPD Points. Please invite your fellow colleagues in the industry. You do not need to be a member to register!

To immediately register: https://www.iafci.co.za/index.php/registration

More information: https://www.broadcastliveevents.com/