THE SAICB REPORT

SOUTH AFRICAN INSURANCE CRIME BUREAU

ISSUE 06: 2011

JULY 2011

INFORMATION UPDATE:

The following information reflects the lists handled for July 2011:

DRäGER
Lists: 3
Records: 462
Hits: 131

TRACKER
Lists: 14
Records: 402
Hits: 146

SAPS13
Lists: 24
Records: 669
Hits: 183

ENQUIRIES
Enquiries:58
Replies:266

INSIDE THIS ISSUE...

SAICB UPDATE

SAICB UPDATE

The new financial year has began and the renovations at the SAICB have been completed. The appointment of the new Data Specialist has been finalized and the new employee will begin in August 2011. The SAICB would like to welcome our latest member as of 1 July 2011—**ALEXANDER FORBES** to the bureau.

July began with the arrest of the main suspect in one of our ongoing cases, which bodes well for the year ahead. Estimated loss incurred by members currently R1 million.

History of the case:
An investigator from the SAICB received a tip-off with information that an individual submitted a false claim for a Laptop and camera with approximate value R17 700.00, that was stolen when his vehicle was broken into.

The ID number that was used in the claim did not match the person claiming, the claim and the bank account that were used were found to have been used for various other claims by various other individuals as well. On 6 July 2011 an operation meeting with the Organised Crime Unit of Germiston and members from SAICB was held in Pretoria to arrest the target.

The target was contacted to arrange for the delivery of a gift voucher by courier. Members from the OCU acted as delivery agents and members from SAICB were in the backup team. The target arrived and was identified by members of SAICB and he was arrested.

The cell phone number that was used by the target was contacted and the phone was not with the target and he did not want to inform the team where his vehicle was parked. On the way to his residential address the vehicle was spotted and a search was conducted and a cell phone was confiscated, this was not the cell phone that the target had used to contact the team.

The team then moved to the targets residential address, at this address the cell phone was found that was used to contact the members from OCU. This phone was hidden in a box in his bedroom. A search and seizure was conducted and the following items, inter alia were confiscated:

FRAUDLINE

In June 2011, **18** reports were received of which **12** reports were for the short term insurance industry, **3** report was received for Brokers and **3** reports for the life industry.

Since 2002, **27159** reports have been received of which **921** reports were for the short term industry **139** reports for the brokers and **39** reports were for the life industry.

For further information on the statistics, please contact Melanie Pillay on melaniep@saicb.co.za

Insurance Fraudline
0860 002526
insurance@fraudline.co.za

MEMBERS

SANTAM

MUTUAL & FEDERAL

HOLLARD

LION OF AFRICA

REGENT

TELESURE

ABSA INSURANCE

STANDARD BANK INSURANCE

OUTSURANCE

MOMENTUM

MIWAY

ALEXANDER FORBES

PARTNERS

SOUTH AFRICAN INSURANCE ASSOCIATION (SAIA)

TRANSUNION

FRAUDLINE

MEMEX

SAFPS

UNICODE

BACSA

NEWORDER

DATADOT

CGC

SAVRALA

SAICB UPDATE *CONT...*

38 cell phones; 50 sim cards; 4 laptops; ID documents for 69 persons identified in the investigation; letters to different banks giving the target permission to use the bank accounts; 150 Policy documents to date; invoices and quotes.

There were policy documents found from a member company in unopened mail, in the name of another alias used by the target. It is clear that further policies and claims will be identified as boxes full of exhibits were confiscated.

Modus Operandi:
The suspect used unsuspecting valid peoples ID numbers and opened insurance policies in their names with the same bank accounts and PO Box numbers. After investigation it was found that the risk addresses that were used did not exist. He phoned the insurance company and lodged a claim and when the assessor tried to contact him to assess the claim they would not be able to get a hold of him. He would phone after a month and berate them for the slow service, the claim was then settled expeditiously.

The search and seizure and subsequent investigation revealed that the suspect had moved from the modus operandi described to cell phone fraud. The suspect bought cell phones from one company and insured them through the shop the phone was bought from. He then lodged a claim and returned to the original store asking to be paid cash for the phone as he had already replaced the missing / damaged phone. The suspect produced invoices for the same phones bought from another supplier on multiple claims.

Further updates and arrests on this and our other cases will appear in future issues.

Vacancies
The SAICB is looking to appoint an Office Manager / PRO and will welcome CV's for this position. Please contact Melanie Pillay on melaniep@saicb.co.za for further information and remuneration package—see page 7 for the Job Description.

In this Issue…
The SAICB recently met with the FBI regarding one of their initiatives in Africa, relating to data security and the current spate of hacking into secure systems experienced internationally. The SAICB has covered this topic extensively in recent Newsletters. As part of their education initiative, the FBI will be contributing information on cyber security and the latest information on cyber criminals to the SAICB Newsletter on an ongoing basis.

The SAICB has agreed to participate in their efforts to address this worldwide problem and will include regular updates on what is being discussed and addressed. The first contribution appears on page 5.

The article that appears on page 3, relates to the progress the UKIFB has made in the UK regarding addressing insurance fraud in the country. The article reiterates the importance of cooperation between the various role players in tackling the issue of insurance fraud and crime, and what can be accomplished when everyone works towards the same goal.

The SAICB always welcomes your feedback on our initiatives and the Newsletter, for us to be able to develop and address any issues arising. So your if you have feedback and /or suggestions , please feel free to contact me on—melaniep@saicb.co.za

ARTICLE—UKIFB

POLICE AND INSURANCE INDUSTRY JOIN FORCES TO CREAT SPECIALIST UNIT TO TACKLE FRAUD

A specialist police unit dedicated to combating insurance fraud is to be set-up through a police-private sector partnership. Funded by the insurance industry and supported by the National Fraud Authority, the unit will be operated by the City of London Police's Economic Crime Directorate.

It will provide additional operational capability to the Directorate, focusing solely on tackling insurance fraud, a crime valued at £2 billion per year – which adds an extra £44 a year to each premium paid by consumers.

The unit, which aims to go live on 1st January 2012, will consist of 35 specialist fraud detectives and police support staff and will provide a dedicated response to threats posed to the insurance industry by both organised gangs and opportunist fraudsters.

The key focus of the unit will be enforcement and prevention strategies designed to tackle current issues. This will be achieved working in collaboration with the City of London Police's National Fraud Intelligence Bureau (NFIB) and the industry funded Insurance Fraud Bureau (IFB).

Whilst embedded within the force's Economic Crime Directorate, the unit will be able to capitalise on the City of London Police's wider policing resources as well as its status as the national lead force for fraud, enabling it to co-ordinate support from UK law enforcement and assist individual forces with their own insurance fraud investigations.

The unit will also work in close partnership with the insurance industry on their continued campaign to prevent insurance fraud and recover the proceeds of crime.

The unit will be funded for the next three years by members of the Association of British Insurers (ABI), and will be subject to an evaluation after two years.

A strategic board containing representatives from the City of London Police, ABI, National Fraud Authority (NFA) and Insurance Fraud Bureau (IFB) will meet quarterly to set priorities for the unit informed by an annual threat assessment and analysis of insurance fraud trends.

The unit builds on the operating model established for the Dedicated Cheque and Plastic Card Unit (DCPCU) where the priorities are set by industry, performance is transparent and reviewed regularly but the operational independence of the police is preserved.

The DCPCU's unique bank-sponsored police squad contains officers seconded from the City of London Police and the Metropolitan Police, and in the nine years since its formation has successfully targeted organised crime gangs and saved an estimated £370 million.

Today's (Jul 12) announcement will strengthen the UK's counter fraud commitment and comes at a time when overall fraud is estimated to cost the UK £38 billion.

The City of London Police sees this as positive step forward in building closer relationships between policing and the private sector, paving the way for other specialist units and, potentially, national economic crime teams to be created through similar funding arrangements in other sectors.

ARTICLE— UKIFB *CONT...*

Confirmation of the unit came days after the ABI revealed it was setting up an Insurance Fraud Register to maintain details of known insurance fraudsters and identify anyone who fails to declare a previous fraudulent claim.

The Commissioner of the City of London Police, Adrian Leppard, said: "A dedicated police unit funded by the insurance industry and operated by fraud detectives from the City of London Police is a major step forward in the fight against a crime that hits the pockets of everyone paying insurance premiums.

"This initiative is the culmination of months of hard work with the insurance industry, and represents another important landmark for private sector funding in policing, something that we should actively encourage within the current financial climate.

"The banking industry has been rewarded for its investment in combating payment card fraud, with savings of £370 million in the past eight years. I now look forward to working with the ABI, IFB and the NFA to ensure the insurance industry benefits in the same way from funding its own specialist police unit.

Home Office Minister for Crime and Security, James Brokenshire, said: "Fraud costs the UK around £38 billion a year, can have devastating consequences and is often used to fund terrorism, drugs and human trafficking.

"The government is determined to give greater focus to tackling both serious and economic crime which is why the powerful new National Crime Agency will ensure we have an improved capability to tackle this issue.

"This will be a great example of how collaborative working can help to combat fraudsters and I want to congratulate and thank the insurance industry and City of London Police for all their hard work and dedication."

David Neave, Chairman of the Insurance Fraud Bureau, (IFB) said: "This strategic step is further evidence of the investment and commitment by the insurance industry in combating fraud.

"The IFB welcomes the opportunity to support this important industry initiative, by working collaboratively with insurers, City of London Police, ABI and NFA, to bring fraudsters to justice and protect the interests of genuine consumers in the process".

Dr Bernard Herdan, CEO of the National Fraud Authority, said: "I welcome these very significant developments and congratulate the insurance industry for funding them. This clearly shows the insurance industry responding positively and creatively in tackling fraud and setting an example from which I hope others can learn.

"This is a great achievement by all the parties involved – the NFA, City of London Police, ABI, IFB and the individual insurance companies who have participated. I am confident the unit will make a significant impact on insurance fraud benefiting the industry and its customers."

Notes:
The City of London Police is the national lead force for fraud, which allows it to investigate fraud throughout England and Wales. It has the largest specialised economic crime team of any police force and provides important national capabilities such as the National Fraud Intelligence Bureau.

The Insurance Fraud Bureau (IFB) is a non-profit organisation funded by the insurance industry. It is specifically focused on detecting and preventing organised and cross industry insurance fraud.

The ABI is the voice of the UK's insurance, investment and long-term savings industry. It has over 300 members, which to-

ARTICLE—UKIFB *CONT...*

gether account for around 90% of premiums in the UK domestic market. The ABI's role is to:

- Be the voice of the UK insurance industry, leading debate and speaking up for insurers.
- Represent the UK insurance industry to government, regulators and policy makers in the UK, EU and internationally, driving effective public policy and regulation.
- Advocate high standards of customer service within the industry and provide useful information to the public about insurance.
- Promote the benefits of insurance to the government, regulators, policy makers and the public.

The UK insurance industry is the third largest in the world and the largest in Europe. It is a vital part of the UK economy, managing investments amounting to 24% of the UK's net worth and contributing the fourth highest corporation tax of any sector. Employing over 275,000 people in the UK alone, the insurance industry is also one of this country's major exporters, with a fifth of its net premium income coming from overseas business.

Insurance and businesses protect themselves against the everyday risks they face, enabling people to own their own homes, travel overseas, provide for a financially secure future and run businesses. Insurance underpins a healthy and prosperous society, enabling businesses and individuals to thrive, safe in the knowledge that problems can be handled and risks carefully managed. Every day, our members pay out £155 million in benefits to pensioners and long-term savers as well as £58 million in general insurance claims.

ENDS

For further information please contact Harry Watkinson at the City of London Police
Press Office on 020 7601 2220, or email:
HARRY.WATKINSON@CITYOFLONDON.POLICE.UK

ARTICLE— FBI

CYBER CRIMINALS TARGETING SMARTPHONE USERS FOR PERSONAL GAIN

Over the last few years, advancements in mobile technology have had significant impacts on the lives of many South Africans. Smartphones, mobile applications, and mobile Internet have provided instant access to data and services that changed the way people engage in education, health, agriculture and banking, to name a few. While these devices and products provide broader and quicker access to required data and services, they significantly increase the user's exposure to cyber threats and cyber criminals.

Recently, the FBI has noticed an increase in cyber criminals targeting smartphones for malicious purposes. Cyber criminals are exploiting the smartphone mobile application markets to distribute malicious applications (apps) that contain malicious software designed to steal personal information or use the phones to engage in illegal activities. Similar to legitimate apps that request user permission to access network communications and hardware controls, the malicious apps request user permission to access certain features of the phone. However, unlike legitimate apps, which request access to limited features and only for user convenience or marketing purposes, the malicious apps request access to the phone state, storage, user identification, and device features via third-party applications that would allow theft of personal information. Third-party applications are used for communications, gaming, social networking, entertainment, and a range of other functions.

- Smartphones have created an opportunity for cyber criminals to exploit the device similar to how personal computers

ARTICLE—FBI *CONT...*

CYBER TERMS

Smartphone: A mobile communication device that offers users expanded capabilities from traditional mobile devices. The features can include text messaging, e-mail access, Internet browsing, and mobile operating systems that enable incorporation of third-party applications to offer even more expanded features.

Android Market: An app called Market is pre-installed on most Android devices and allows users to browse and download apps published by third-party developers and search and read detailed information about the apps from the Android Market Web site.

Trojan: A useful, or seemingly useful, program that contains hidden code of a malicious nature.

Botnet: A network of computers that run autonomously and are controlled by a command-and-control (C&C) computer or network of computers.

Spam: A slang term for unsolicited commercial e-mail messages or junk mail.

IMEI: International Mobile Equipment Identity; a unique identity number given to mobile phones. This number can be used to block mobile phones that have been stolen when reported to the network operator.

IMSI: International Mobile Subscriber Identification; an internal subscriber identity used only by the network.

Short Message Service (SMS): The transmission of short text messages or live chats to and from a mobile phone. Messages must be no longer than 10 alphanumeric characters and contain no images or graphics.

Malware: Malicious software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse.

(PCs) are targeted. Similar to PCs, smartphones are mini-computers that allow users to check e-mail, browse the Internet, and store a large amount of personal information like passport numbers, access codes, PINs and account information for online banking, and other high-valued data.DroidDream is a Trojan that is able to obtain sensitive data, such as International Mobile Equipment Identity (IMEI) and International Mobile Subscriber Identification (IMSI) numbers, from an infected device and download additional malicious code to the phone from remote servers.

- The Trojan-SMS malware-(Trojan-SMS.AndroidOS.FakePlayer.a)-is being distributed through an unknown Website and is hidden inside a movie player app. When downloaded the app requests user permissions to access storage, phone calls, and send text messages to premium-rate numbers without the owners' knowledge.

Open source reporting has identified other malicious software that request access to personal information, messages, contact lists, and other phone features that would allow the phones to send information or receive commands to engage in crimes, such as spam and attacks.

- In February 2011, Symantec, a recognized leader in security software, reported that it had detected an Android Trojan (Android.Pjapps) that aimed to build a botnet controlled by a number of different C&C servers. The Trojan is able to install apps, navigate to Web sites, add bookmarks to the browser, send text messages, and block text message responses. The Trojan is hosted on a Chinese Web site and sends sensitive information from the device to include IMEI, Device IS, Line Number, and Subscriber ID.

- In February 2011, Lookout Mobile Security identified another Android Trojan, Hong Tou Tou (a.k.a. ADRD), that requests user permission to turn the phone on or off and turn on and use the Internet. Once installed, the app sends encrypted data with the phone's IMEI and IMSI to a remote server and receives a set of search engine targets. The search engine targets are capable of processing commands instructing it to download a file that could allow the malware to monitor SMS conversations and insert content related to specific keywords into the SMS conversation, though this has not been observed.

ARTICLE— FBI *CONT…*

- Lookout Mobile Security identified a more enhanced Android Trojan-Geinimi-with botnet-like capabilities. Geinimi is being distributed through third-party Chinese app stores as repackaged versions of legitimate apps, mainly games, and accepts commands from a server controlled by an unknown party. Geinimi requests permissions to call the phone, read, write, send, and receive SMS messages, read and write bookmarks, and access the Global Positioning System.

With the growing number of individuals using mobile devices, it is very likely that cyber criminals will continue targeting smartphones to collect sensitive information, relying on most users' lack of knowledge on how to secure data on these devices unless users begin practicing better phone security.

Thank you the Cyber Intelligence Section of the FBI for this article. For more information contact (202) 651-3090 or visit their website—www.fbi.gov

ARTICLE—VACANCY

JOB DESCRIPTION: OFFICE MANAGER / PRO

PURPOSE OF THE POSITION

The Office Manager is responsible for organising and coordinating all office operations and procedures in order to ensure organisational effectiveness and efficiency.

The PRO role will include being responsible for the image and reputation of the SAICB, while promoting and informing all role players, stakeholders, industry and public about the SAICB and its role/successes etc.

SCOPE

The Office Manager / PRO will report to and work closely with Chief Operating Officer and be responsible for providing among other roles, office management services which includes maintaining office services and efficiency, supervising office staff and maintaining office records.

RESPONSIBILITIES

Major responsibilities and target accomplishments of the position:

Maintain office services

Main Activities: Design and implement office policies; Establish standards and procedures; Organise office operations and procedures; Supervise office support staff; Review and approve supply requisitions; Liaise with other agencies, organisations and groups; Oversee the maintenance of office equipment

Supervise office staff

Main Activities: Assign and monitor clerical and secretarial functions; Orient and train support staff; Provide on the job and other training opportunities; Assist with the evaluation of staff performance; Coaching and disciplining staff; Responsible for implementing the process to appoint new staff – Guidelines on Interview processes. Monitors that correct documentation is

ARTICLE—VACANCY *CONT...*

completed and the correct procedures followed; Responsible for induction program for new staff; Maintains the Staff Manual make sure that any changes are brought to the attention of all staff ; Monitors the staff leave register to make sure that they adhere to the relevant laws and SAICB staff rules; Skills Development Facilitator: completing Workplace Skills Plan and Annual Training Report for Inseta; Oversee the training programme; Performance Plan and implement Appraisal System – implementation of this system to be able to identify training needs and to monitor the performance of staff (this is an ongoing process); Run a monthly staff meeting to facilitate the transfer of information relating to issues affecting staff or SAICB procedures – is sometimes also used as training opportunity (general or specific); Staff salaries process.

Maintain office records

Main Activities: Oversee filing systems; Design templates; Ensure filing systems are maintained and up to date; Define procedures for record retention; Ensure protection and security of files and records; Ensure effective transfer of files and records Transfer and dispose records according to retention schedules and policies; Ensure personnel files are up to date and secure;.

Infrastructure

Liaise with building management regarding office matters e.g. parking, air conditioning, security etc.; Oversee the administrative process for purchasing new furniture as well as the selling thereof; Manage and supervise the Receptionist/switchboard operator; Responsible for all telephone related issues; Supervises all kitchen related issues.

PRO and other duties

Design, write and maintain website; Facilitate Board meetings and committee meetings and procedures; Prepare Board packs for meetings; Prepare agendas and take minutes for meetings; Ensure meeting outcomes are met; Plan and facilitate actual meetings; Design and facilitate the sending out of information and managing the resultant correspondence. Develop and maintain relationships with relevant stakeholders and organizations; Write media releases and articles related to the organization. Assist with queries. Assist COO. Manage the Board, EXCO and SPOC committee meetings; Notification of meetings

Drawing up of letter to call for nominations for new board; Compiling list of nominees and inform members; Drawing up of relevant documentation e.g. Draft Agenda, Proxy forms, Ballot Paper, Score sheet; Make sure that all documentation is done and distributed according to timelines and other procedures defined in the Association Agreement; Prepare document packs for the meetings; Finalise the counting of the ballot papers – advise chairman of final outcome; Responsible for new member application process – do all the administration; Manages process when members resign; Authorised signatory - order forms to be completed for any purchase .

Performs any other duty, which is in keeping with the profile of the job and which may reasonably be expected from the staff member, as directed by their Manager or member of the SAICB Executive.

Please contact Melanie Pillay on melaniep@saicb.co.za for further information and remuneration package.

CONTACT

For further information or if you wish to reproduce any of the articles in this Newsletter, please contact :
Hugo van Zyl on hugovz@saicb.co.za or Melanie Pillay on melaniep@saicb.co.za