UNIVERSITY OF CAPE TOWN
IYUNIVESITHI YASEKAPA • UNIVERSITEIT VAN KAAPSTAD

FINANCE DEPARTMENT
Unleashing finance expertise

A quick guide to Fraud Prevention

A informative guide to assist in the prevention of fraud and corruption.

Unleash human potential for a fair and just society
UCT Vision 2030

www.uct.ac.za

Fraud and corruption

Fraud is the use of deception with the intention of obtaining personal gain, avoiding an obligation or causing loss to another party. Fraud can be used to describe a wide variety of dishonest behaviour such as forgery, false representation and the concealment of material facts.

Fraud, and the harm it causes, is not a new issue for the University, it is one that is constantly changing. Fraudsters do not recognise organisational boundaries and those who fight fraud often must work across organisational boundaries to find fraud and bring those who commit it to account.

Fighting fraud and corruption has always been an area where collaboration is key to make sure we are dealing with fraud and corruption with the best practices and tools at our disposal. Addressing fraud needs a holistic response incorporating detection, prevention and redress, underpinned by a strong understanding of risk.

Who is this guide for?

This guide is intended to inform and assist the staff of the University of Cape Town in dealing with and preventing fraud.

#WISEUPWATCHOUT

Important contacts

Whistle Blowers 24 Hour Hotline:

call **0860 650 000**

or SMS **33490**

uct@whistleblowing.co.za
www.whistleblowing.co.za

Accepted principles

- There is always going to be fraud.
- Finding fraud is a good thing.
- There is no one solution.
- Fraud and corruption are ever changing.
- Prevention is the most effective way to address fraud and corruption.

Preventing fraud via:

Awareness: We will raise awareness of fraud and its safeguards among our partner organisations and our stakeholders.

Prevention: We will improve our systems and controls to support our business.

Teamwork: We will remove silos and work together across Faculties and Departments to share information and develop combined approaches to countering fraud.

Investigation: We will be proactive in analysing data to identify areas at risk. We will be effective and professional in our investigations of specific cases and maintain a robust whistle blowing procedure.

Enforcement: We will continue to be tough on fraudsters by punishing them efficiently and effectively.

What you can do

Your role as a member of staff is to establish an effective counter fraud culture by:

- Engaging and being alert to the risk of external and internal fraud;
- Identifying suspicious activities and control weaknesses; and
- Reporting any suspicions quickly and appropriately.

UCT HAS A ZERO TOLERANCE APPROACH TO FRAUD

THERE IS NO ACCEPTABLE LEVEL OF FRAUD !

Zero-tolerance culture

We aim to ensure that a zero-tolerance culture to fraud is maintained and that fraud is effectively managed at all levels of UCT's service delivery as follows:

- Supporting all staff in their responsibilities in preventing and detecting fraud through guidance and training;
- Providing managers with specialist support in designing, operating and reviewing internal controls;
- Maintaining comprehensive procedures for preventing and detecting fraud that must be carefully followed and monitored;
- Protecting members of staff through a robust process for reporting suspicions of fraud;
- Using data and technology efficiently in the systems in place to combat fraud; and
- Sharing knowledge of vulnerabilities and lessons learned through strong communication channels.

PCard ATM fraud

- If you think the ATM is faulty cancel the transaction IMMEDIATELY and report the fault to your Bank. Transact at another ATM. Toll free numbers are displayed on all ATMs.
- Don't use ATMs where the card slot, keypad or screen has been tampered with. It could be an attempt to get hold of your card.
- Have your card ready in your hand before you approach the ATM to avoid opening your purse, bag or wallet while in the queue.
- Be cautious of strangers offering to help as they could be trying to distract you in order to get your card or PIN. Take note that fraudsters are often well dressed, well-spoken and respectable looking individuals.
- Should you have been disturbed whilst transacting, immediately change your PIN or stop the card, to protect yourself from any illegal transactions occurring on your account.
- Memorise your PIN, never write it down or share it with anyone, not even with your family member or a Bank official.
- Choose a PIN that will not be easily guessed. Do not use your date of birth as a PIN. Key your PIN in personally in such a way that no one else can see it, e.g. cover your hand when you key in your PIN, even when alone at the ATM as some criminals may place secret cameras to observe your PIN.

ABSA	0800 111 155
African Bank	0861 000 555
Bidvest Bank	0860 111 177
Capitec Bank	0860 102 043
FNB	0800 110 132
Nedbank	0800 110 925
Standard Bank	0800 020 600

Phishing

Phishing comes in the form of unsolicited emails appearing to come from a reliable sources like the bank, SARS or your email service provider.

You are directed to click on a hyperlink or icon to view or submit information. Once clicked, the link diverts the victim to a fraudulent website where any information entered will be sent to the fraudsters.

The information requested is usually personal information and could include usernames and passwords for banking platforms or email accounts as well as cellphone numbers and bank card details. Clicking on the link or icon could also result in the victim's computer being infected with malware.

- Do not click on links or icons in unsolicited emails.
- Do not reply to these emails. Delete them immediately.
- Do not believe the content blindly. If you are concerned use your own contact details to contact the sender to confirm.
- Type in the URL for your bank in the internet browser if you need to access your bank's webpage.
- Check that you are on the real site before using any personal information.
- If you think that you might have compromised yourself, contact your bank immediately.

Red flags for Line Managers

- Unwillingness to share duties;
- Refusal to take leave;
- Refusal to implement internal controls (e.g. skipping approvals; segregation of duties.);
- Replacing existing suppliers with suppliers that have an unusually close connection;
- Failure to keep records or receipts;
- Bullying colleagues (especially if the colleagues question the person's activities);
- Past legal/compliance problems;
- Abnormally high costs in a specific cost centre function;
- Reconciliations not performed on a reg-ular basis;
- Payments continuously just below re-porting thresholds;
- Duplicate invoices and sequential numbers on invoices;
- Pricing does not adjust with changes in the value of goods or services in the market; and
- Owners of company not identifiable.

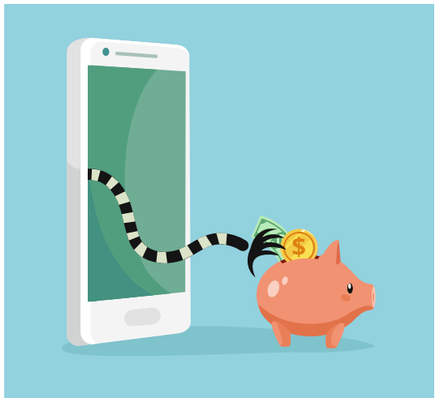
Internet purchasing tips

- Only make purchases with your PCard on reputable websites that are verified as secure sites.
- When receiving promotions or special deals via email or telephone or from online websites, always verify the validity of the source before providing your personal and banking details to be debited.
- Do not send emails that contain personal information such as your card number and expiry date.
- To ensure that you are using a secure shopping site, check for a picture of a closed lock with "verified" or "secure" at the bottom of your screen.

  On the web page, where you enter your credit card or other personal information, look for a lock and an 's' after 'http' in the web address of that page – it should start with: 🔒 **https://**. This indicates the site is encrypted, which is a security measure that scrambles your data as it is entered.

Cellphone banking

- Memorise your PIN, never write it down or share it with anyone.



- Choose an unusual PIN that is hard to guess and change it often.
- Protect your phone content and personal information you saved by using a PIN or Password to access your phone. Do not leave your phone unlocked.
- Do not respond to competition SMS's or MMS's.
- Regularly verify whether the detail received from cell phone notifications is correct and aligns with the recent activity on your account.

What is a 419 scam?

A letter or email is sent to a multitude of recipients making an offer that would result in a large pay off for the recipient ("victim").

Invariably, the victims' banking details as well as sums of money are said to be required in advance in order to facilitate the payment of the funds.

Essentially, the promised money transfer never happens and in addition the fraudsters may use the victims' banking details to withdraw money for themselves.

Beware if:

- The communication sounds too good to be true;
- The promise of large sums of money for little or no effort on your part;
- The victim is requested to provide money upfront as a processing admin fee;
- The request usually contains a sense of urgency;
- The victim does not know the person who has sent the communication;
- The sender requests confidentiality;
- Lottery, inheritance or prize themes are popular in the communications; or
- Payments are requested to be made by MoneyGram.

- In some instances, genuine companies' letterheads are utilised to convince the victim of the authenticity of their request.
- If you receive a scam email, do not reply.
- You can however forward a copy of the email to the Internet Service Provider from where the email originated. For example: abuse@hotmail.com; abuse@yahoo.com; abuse@compuserve.com; etc.
- Forward the email to the South African Police Services (SAPS) at 419scam@saps.org.za.
- If you have fallen victim, immediately contact SAPS.

How does a deposit and refund scam happen?

A criminal orders goods or services from a business and makes a payment into the victims account.

The order is cancelled, and an urgent refund is requested, alternatively a payment is made in "error" and an urgent refund is requested.

- No "refund" should be made without first verifying with the bank that the deposit that has been made into your account is indeed valid.
- In addition, wait for all deposits to first be cleared.
- Staff dealing with finances in your organisation should be educated about such scams.

Vendor banking details

All changes to vendor bank details must be supported by an original letter from the relevant bank.

In circumstances where this is not possible further due diligence will be applied by the University in consultation with the relevant bank and applicant to ensure correctness and legitimacy.

Partnership in fraud prevention

Preventive controls are designed to limit the possibility of a fraud occurring e.g. separation of duties.

Detective controls are designed to spot errors, omissions and fraud after the event e.g. supervisory checks and reconciliations.

Support for managers in establishing appropriate controls is provided by the appropriate finance business partners and internal audit.

All cases of actual or suspected fraud will be vigorously and promptly investigated and appropriate action will be taken.

The police will be informed where con-sidered appropriate.

In addition, disciplinary action will be considered not only against those members of staff found to have perpetrated frauds but also against managers whose negligence is held to have facilitated frauds.

Both categories of offence can be held to constitute gross misconduct, the penalty for which may include summary dismissal.

Who to contact

The first point of call would be to re-port any suspicious activity to the Whistle Blowers 24 hour hotline. These calls will be passed onto the Compli-ance and Risk Management team.

This will ensure an independent, unbiased assessment is done and, specifically when a staff member wants to report on a line manager, it is anonymous and without potential victimisation from the line manager.

#WISEUPWATCHOUT

SPEAK UP NOW!

ILLEGAL AND UNETHICAL CONDUCT
ABUSE OF UNIVERSITY ASSETS
BRIBERY AND CORRUPTION
EXAM IRREGULARITIES
THEFT AND FRAUD

WHISTLE BLOWERS

PRIVATE & CONFIDENTIAL

0800 650 000

SMS 33490
uct@whistleblowing.co.za
www.whistleblowing.co.za