X12

FINDINGS REPORT CYL2586

Data Acquisition and Analysis Pertaining to

MiWay

25 July 2017

Strictly Private and Confidential

Findings Report

CYL2586 - MiWay

Forensic acquisition performed by	:	Jaco Engelbrecht
Forensic Analysis by	:	Danny Myburgh
Report Compiled by	:	Danny Myburgh
Report Reviewed by	:	Bennie Labuschagne

Confidentiality : This report has been prepared on the request of Mr René Otto, Chief Executive Officer of MiWay Insurance Limited ('MiWay')

Tel: +27 (0) 12 664 0066 Fax: +27 (0) 86 601 4321
244 Jean Avenue, Norma Jean Square, Block 5, Centurion, South Africa
P O Box 10312, Centurion, South Africa, 0046

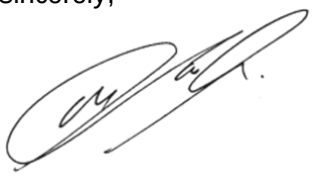
Mr René Otto
Chief Executive Officer
MiWay

25 July 2017

FINDINGS REPORT: CYL2568 - MIWAY

1. In accordance with your instructions, we have the pleasure of presenting our report in the above matter.
2. We require sufficient communication and preparation time prior to testifying in any prosecuting proceeding.
3. If you wish to discuss the contents of this report, please contact Danny Myburgh on or Bennie Labuschagne on 012 664 0066.
4. It is trusted that this information assists you with your investigation.

Sincerely,



Danny Myburgh SCERS, ENCE
MCom - Forensic Accounting, BComHons - Information Systems, Nat Dip (Pol Adm)
Managing Director

1 BACKGROUND

1.1 Cyanre, The Digital Forensic Lab (Cyanre) was instructed by Webber Wentzel on behalf of MiWay, represented by Mr René Otto, to assist with the acquisition and analysis of social media content and e-mail communication.

1.2 For internal purposes the case was designated CYL2568.

1.3 Cyanre was informed that information was published on social media platforms (Twitter and Facebook) on or about Thursday 20 July 2017 purporting to be internal communication of MiWay (For ease of reference hereafter referred to as the publication).

1.4 Due to threats received and possible harm to the individuals mentioned in the publication, Cyanre was requested not to include any more details on individuals other than what is already in the public domain, although these details have been disclosed by MiWay and verified by Cyanre. MiWay verified the identity of "Nobu" as an employee.

1.5 The published information consists of what would seem to be a screen-print taken of an internal e-mail between "Aarthi Roopnarain" from e-mail account AarthiR@miway.co.za and "Nobu" sent on Monday 27 March at 3:26 PM.

1.6 The purported e-mail communication refer to a "manager meeting" which took place on the previous day to the mail, being 26 March 2017, upon which a decision was taken to reject 90% of all claims from black people as from 1 August 2017. Black people were also referred to as "easy targets" and baboons".

1.7 We were informed by MiWay that they utilize Meltwater as their brand monitoring on social media platforms. This system detected the publication on Twitter after which it was reported to the management of MiWay. Personnel of MiWay then accessed the Twitter account of "@ziggymoy" with the display name "Magnanimous".

1.8 Personnel of MiWay used the detail in the publication to identify the MiWay employees allegedly involved. These employees' e-mail folders were searched to locate the e-mail in question. The e-mail as documented in the publication could not be located, but an e-mail, sent on the same date and time (27 March 2017 at 3:26PM) by "Aarthi Roopnarain" was identified. This email was sent to the mail account of djmondlim@gmail.com and was addressed to "Mondli". We have been informed by MiWay that this was ongoing communication on a claim of a client at that time, namely Mr Mondli Madlala.

1.9 Personnel of MiWay used this identity to search for the Facebook profile of this client. Upon locating the profile it was discovered that the publication was seemingly published on the client's Facebook profile prior to the Twitter publication.

1.10 The investigation performed by the employees of MiWay established that no trace of the e-mail, as contained in the publication, existed on MiWay's mail systems. Based on this as well as a number of identified inconsistencies in the published image, the management of MiWay concluded that the publication was manipulated and issued a media statement accordingly.

1.11 We were further informed by MiWay regarding the following aspects:

1.11.1 The persons referred to in the publication being "Aarthi Roopnarain" and "Nobu" are employees of MiWay.

1.11.2 MiWay took screen-prints of the publication both from Twitter and from Facebook.

1.11.3 MiWay is using the Meltwater system for brand monitoring.

1.11.4 MiWay is using Office 365 and Mimecast for all e-mail communication.

1.12 Cyanre was requested to trace the origin of the publication, to fully analyse the publication and determine if it is authentic and compile a report on all the findings.

2 FORENSIC ACQUISITION METHODOLOGY

2.1 On Thursday 20 July 2017 Cyanre was approached by MiWay to assist with the investigation.

2.2 On Friday 21 July 2017, Mr DC Myburgh and Mr Jaco Engelbrecht, from Cyanre, together with a representative of Webber Wentzel attended a meeting held at MiWay's premises at 48 Sterling Road, Samrand Office Park, Kosmosdal, Centurion.

2.3 Mr Myburgh and Mr Engelbrecht was briefed by the management team of MiWay regarding the events which took place as well as the actions taken by staff of MiWay to secure related information.

2.4 Mr Myburgh interviewed the Head of IT infrastructure at MiWay. The mail configuration of MiWay was explained to Cyanre. Mr Myburgh requested the creation of a full download of the mailboxes of the MiWay employees, "Aarthi Roopnarain" and "Nobu". This process was started and allowed to run into the weekend.

2.5 Mr Myburgh also interviewed the Digital Communications Manager at MiWay who explained the brand monitoring methodology and platform used to monitor comments on social media regarding MiWay. Mr Myburgh requested the download of all information relating to this incident, which the brand monitoring equipment recorded. This process was started and allowed to run into the weekend.

2.6 On Monday morning 24 July 2017, Cyanre again attended the MiWay premises and collected a copy of the downloaded information. Upon returning to the offices of Cyanre a forensic copy was created of all the collected data.

3 FINDINGS

3.1 Upon receiving the request for assistance from MiWay, Cyanre accessed the public Facebook account of “Mondli Madlala”, as identified by the MiWay staff. This was done at 19:32 on 20 July 2017. It was determined that the Facebook profile is a valid and active profile and was opened during August 2011. It was further established that the publication in question was already removed from the profile. Cyanre was informed by MiWay that to date they have not publically identified the Facebook profile under which the publication was made or the identity of the client whom they suspect might be responsible for the publication.

3.2 A screen print, which was made of the Twitter thread containing the publication, was obtained as well as a copy of the Twitter publication that was automatically recorded by the Meltwater brand monitoring software used by MiWay. The Meltwater software was inspected by Cyanre and it was established that the software actively monitors content on identified social media platforms. This content is monitored without human intervention and a copy is retained for reviewing purposes even if the original publication is removed or altered. Based on how the software collects and retains online content, as well as verifying the content against the screen-print which was created, it is confirmed that the content recorded is a true reflection of the content of the publication at the time when it was published.

3.3 The following image depicts the content of the publication made on Twitter (A full-page copy is attached as per Annexure A):

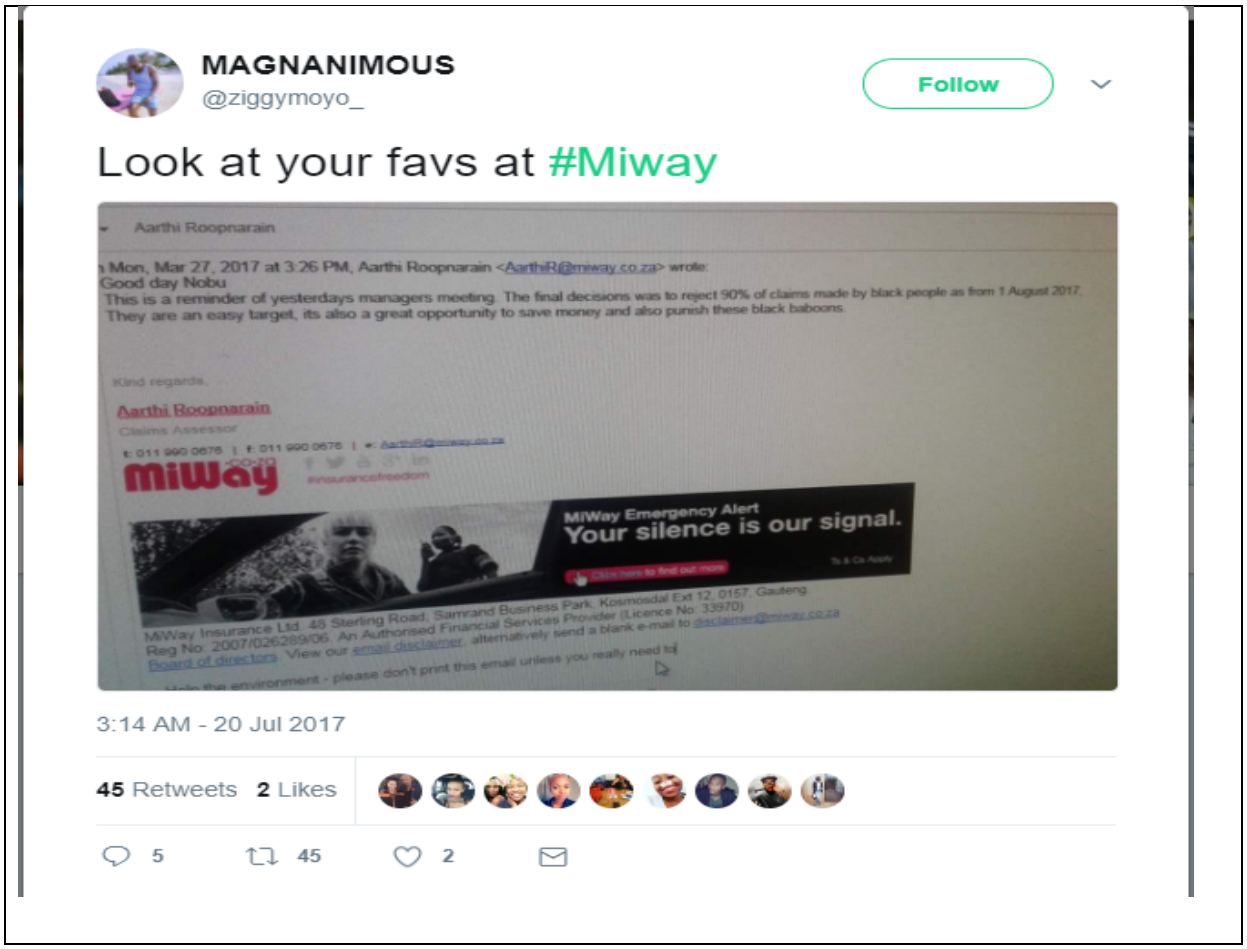


Image 1

3.4 The following image, with added endorsements for reporting purposes, depicts just the content of the publication made on Facebook. (An unedited full-page copy is attached as per Annexure B):

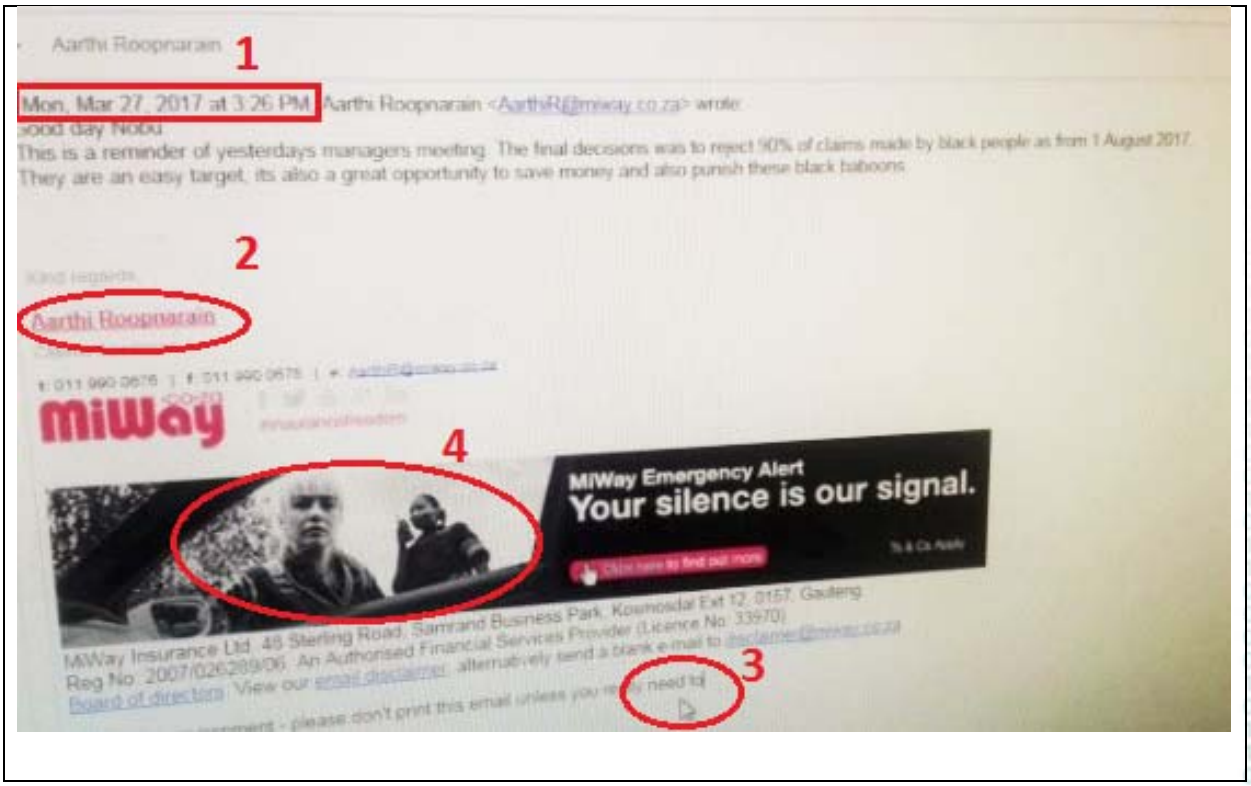


Image 2

3.5 Upon analysing the image the following was observed (please refer to image 2 for the identified aspect):

3.5.1 Aspect 1 - The e-mail was purportedly sent on Monday 27 March 2017 at 3:26PM. It refers to a managers meeting, which was allegedly held on the 26th of March 2017, which was a Sunday. Cyanre was informed by client that neither "Aarthi Roopnarain" nor "Nobu" are managers and that no managers' meeting was held on Sunday 26 March 2017. This information was not confirmed by Cyanre.

3.5.2 Aspect 2 - The spell-check underlined and highlighted in red under the signature name of the sender is not indicative of a mail which was sent and received. This is an inconsistency and indicative of possible manipulation.

3.5.3 Aspect 3 - The cursor at the end of the sentence is indicative of the publication still being in the process of being edited. This is not indicative of a mail, which was sent and received. This is an inconsistency and indicative of possible manipulation. The name "Aarthi Roopnarain" appears at the top of the image in

what appears to be an address tab. The address tab is of the style used in the Gmail internet based email service. It appears that the person who created this screen grab either sought to forward or reply to an email from "Aarthi Roopnarain". This renders the content of the prior email into text which can be freely edited. Before the email was sent, a screen grab was taken.

3.5.4 Aspect 4 - Cyanre was informed by client that the MiWay Marketing banner as displayed in the mail is added by Mimecast on all outgoing mail. Cyanre verified this fact by testing the mail platform of MiWay and found that on internal mails, as the publication purports to be, the following signature banner is added and not the one depicted in the publication (Supporting information from the MiWay e-mail platform Mimecast is attached as per Annexure C):

Image 3

This aspect is not indicative of a mail, which was sent internally, but rather that of a mail which was sent to a person external to MiWay. This is an inconsistency and indicative of possible manipulation.

3.6 Cyanre was informed by MiWay that all internal and external mails are sent via Office 365 and external mails further through Mimecast. Office 365 is an application, which allows for the archiving of all inbound and outbound e-mails. Users are not able to delete or modify any e-mail on this archive platform due to the fact that MiWay has an organisational wide policy enabled on Office 365, namely "Litigation Hold". The platform is therefore tamper proof in the sense that no e-mail can be removed or altered once it was logged in the platform. It also indexes all e-mails to facilitate the accurate search for e-mails. Due to the fact that a user does not have the ability to modify the server settings of Office 365 any e-mail archived will show the true and correct content, date and time when a mail was sent or

received. Further, an independent external third party hosts the platform, which aids in the authenticity of the archived information. More information can be obtained from their official website at https://technet.microsoft.com/en-us/library/ff637980%28v=exchg.160%29.aspx?f=255&MSPPError=-2147217396It. (Supporting information from the MiWay e-mail platform Office 365 is attached as per Annexure D).

3.6.1 It was established that the only mail, sent from the "Aarthi Roopnarain" mail account on 27 March 2017 at 3:26 PM, was sent to the mail account of djmondlim@gmail.com and was addressed to "Mondli". We have been informed by MiWay that this was communication, which was on-going with a client of MiWay, namely Mr Mondli Madlala. The following image depicts the mail which was sent (A full-page copy is attached as per Annexure E):

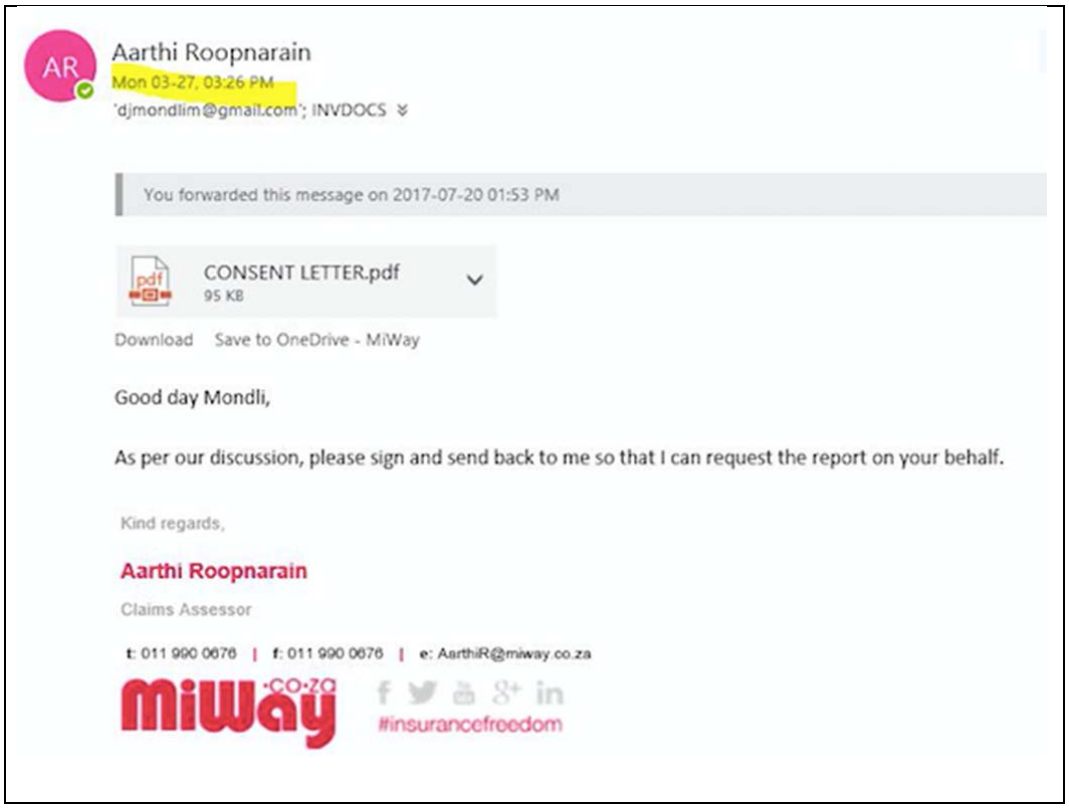


Image 4

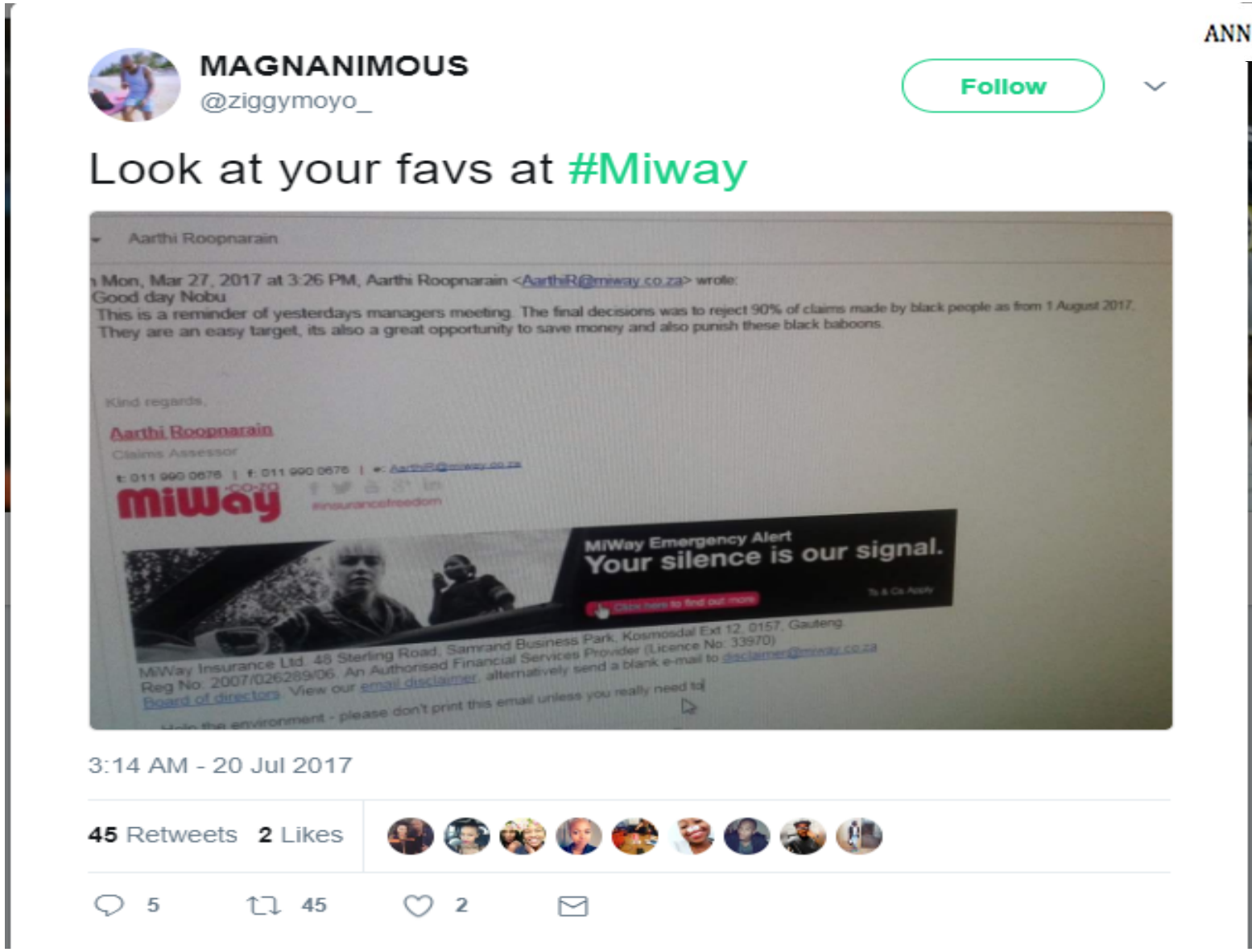
3.6.2 Cyanre performed an extended search across the two e-mail archives of “Aarthi Roopnarain” and “Nobu” to determine if it contained the mail as depicted in the publication to any internal or external party. No traces of the mail could be located.

4 SUMMARY OF FINDINGS

4.1 MiWay utilises Office 365 as an external e-mail platform, which records all incoming and outgoing mail, without allowing the user to remove or modify e-mails. Based on the fact that no trace of the mail contained in the publication could be located on the platform it can safely be concluded that the mail depicted in the publication was not sent from employees of MiWay in the format as published.

4.2 Based on the fact that there are clear indications that the mail was being edited and inconsistencies indicative of manipulation was located, it can safely be concluded that the mail depicted in the publication was manipulated or edited.

4.3 The original e-mail located was sent from the “Aarthi Roopnarain” mail account on 27 March 2017 at 3:26 PM, to the mail account of djmondlim@gmail.com and was addressed to “Mondli”. It was also established that the publication was published on 20 July 2017 on the Facebook profile of “Mondli Madlala”. It is therefore concluded that the owner of the “Mondli Madlala” Facebook profile was the originator of the publication or involved in the publication.



MAGNANIMOUS
@ziggymoyo_

Follow

Look at your favs at #Miway

Aarthi Roopnarain

Mon, Mar 27, 2017 at 3:26 PM, Aarthi Roopnarain <AarthiR@miway.co.za> wrote:
Good day Nobu
This is a reminder of yesterdays managers meeting. The final decisions was to reject 90% of claims made by black people as from 1 August 2017.
They are an easy target, its also a great opportunity to save money and also punish these black baboons.

Kind regards,

Aarthi Roopnarain
Claims Assessor
t: 011 990 0676 | f: 011 990 0676 | e: AarthiR@miway.co.za

MiWay
#insurancefreedom

MiWay Emergency Alert
Your silence is our signal.
Click here to find out more
Ts & Cs Apply

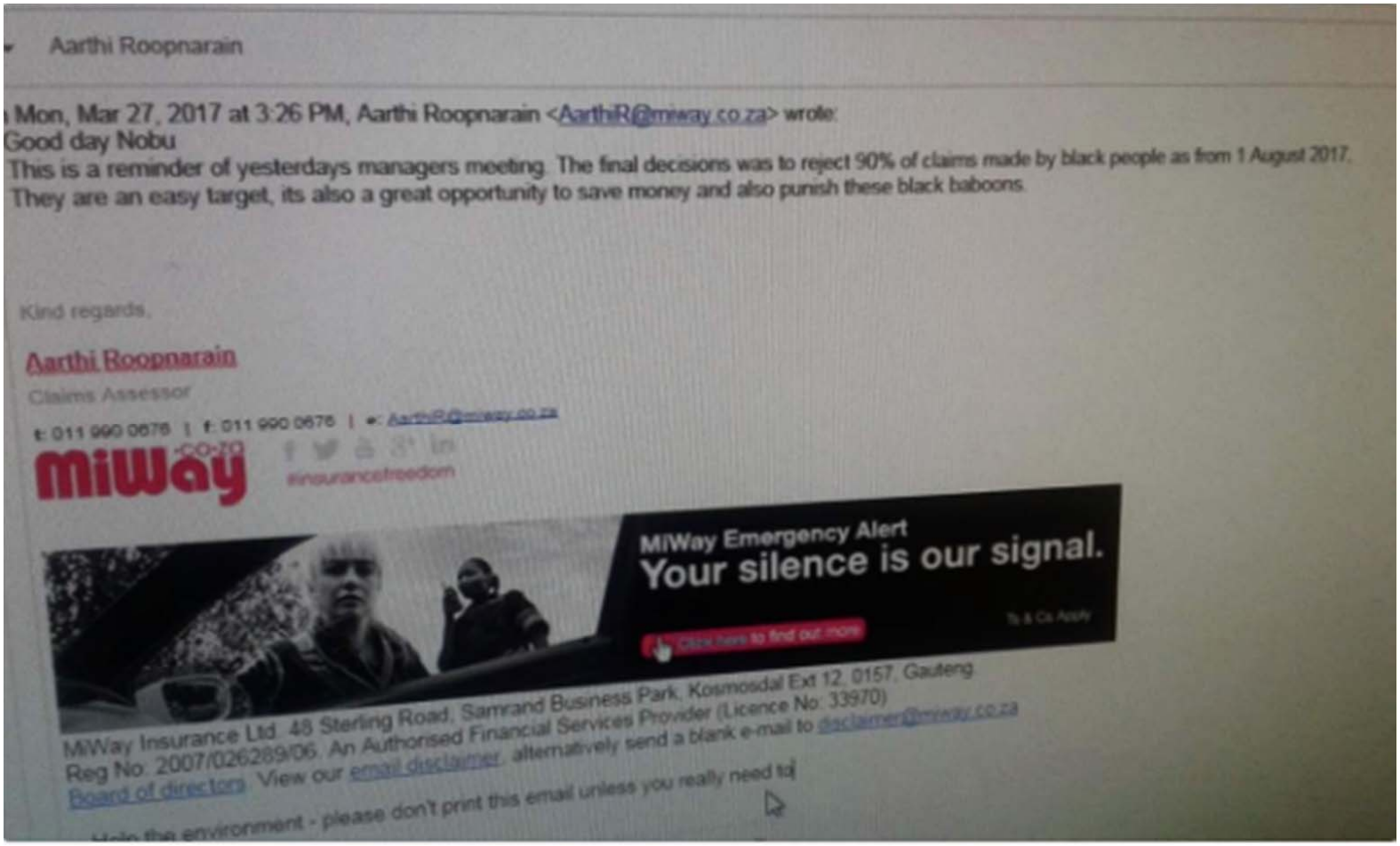
MiWay Insurance Ltd. 48 Sterling Road, Samrand Business Park, Kosmosdal Ext 12, 0157, Gauteng.
Reg No: 2007/026289/06. An Authorised Financial Services Provider (Licence No: 33970)
Board of directors. View our email disclaimer, alternatively send a blank e-mail to disclaimer@miway.co.za

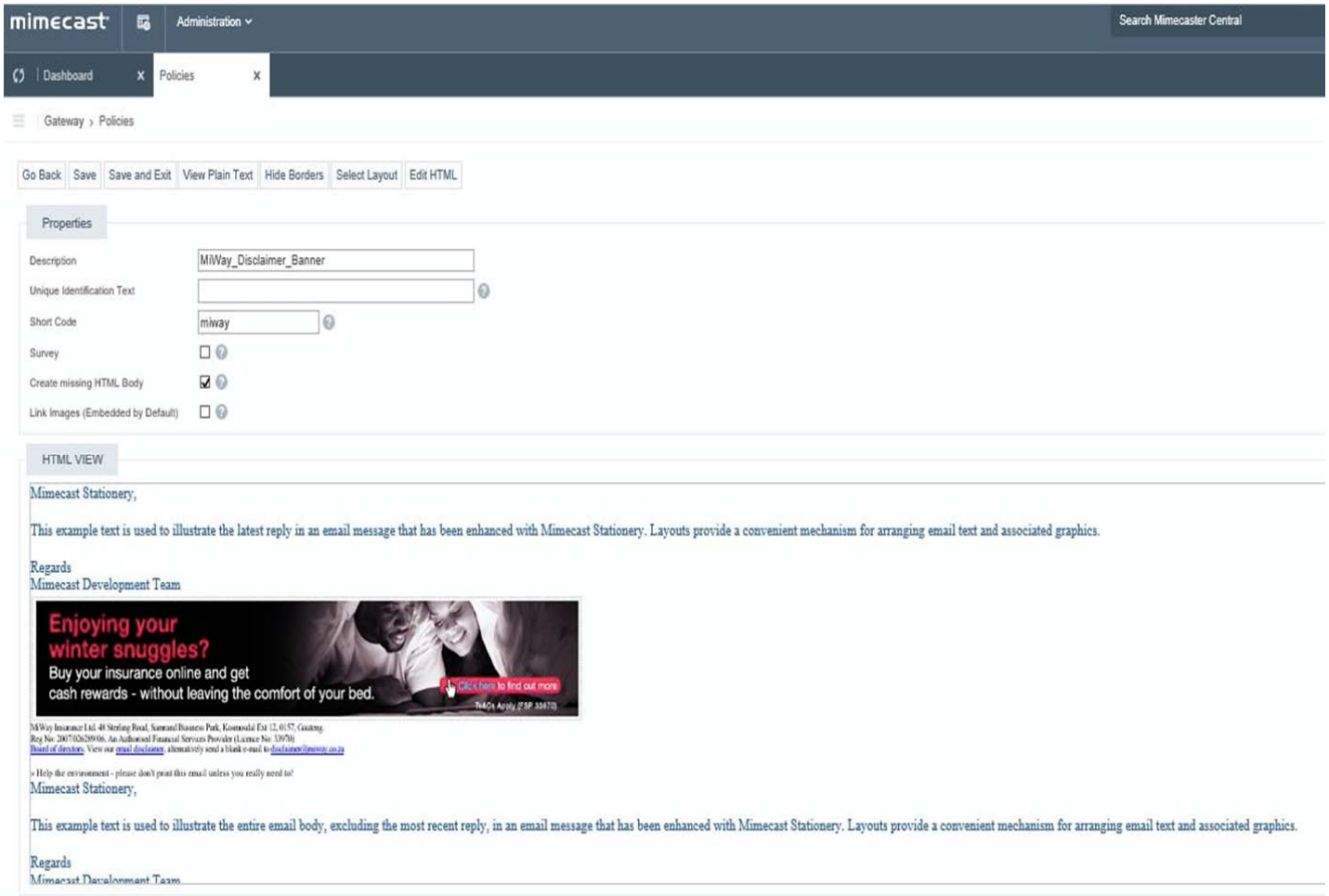
Help the environment - please don't print this email unless you really need to

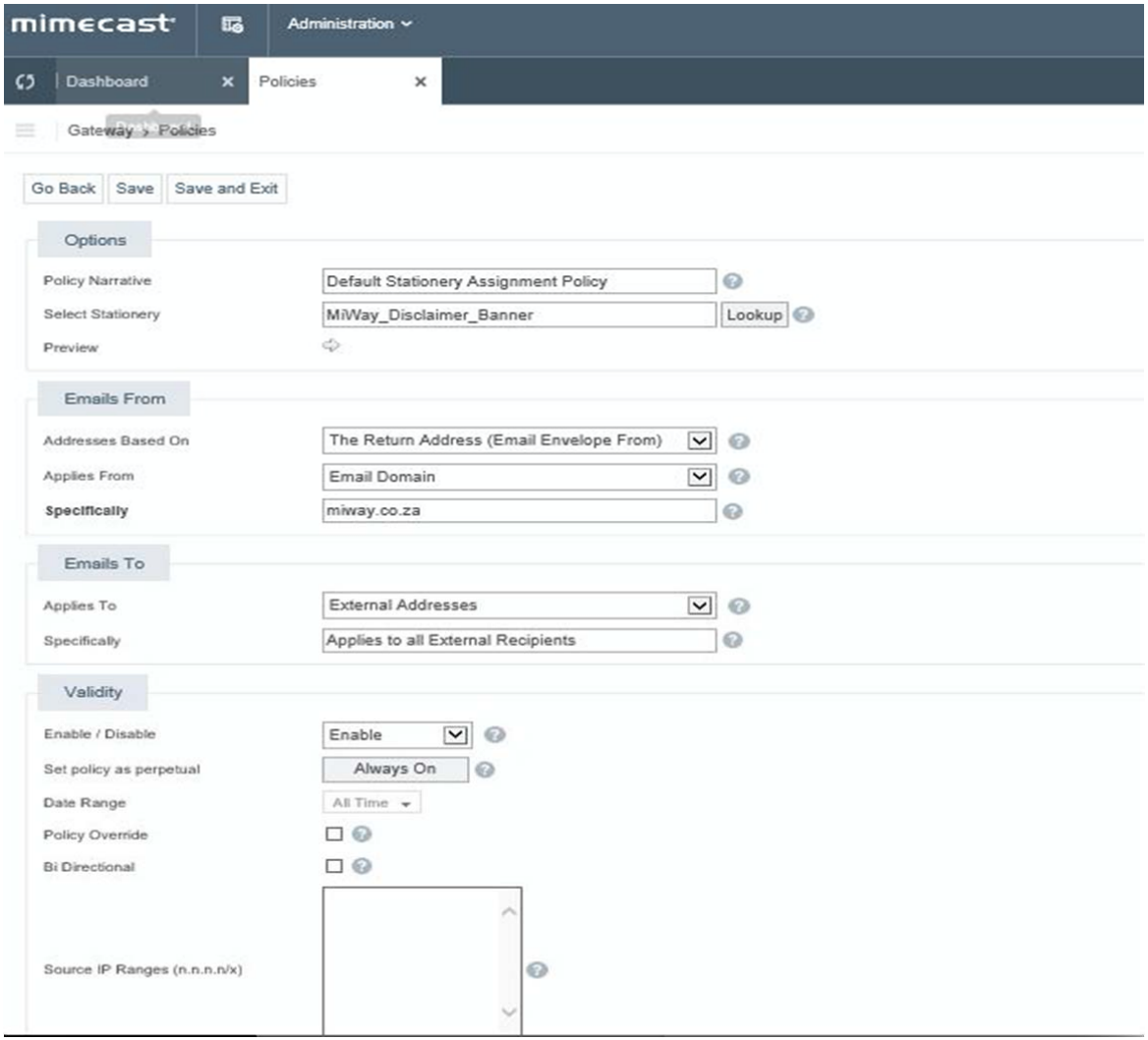
3:14 AM - 20 Jul 2017

45 Retweets **2** Likes

5 45 2


Aarthi Roopnarain
Mon, Mar 27, 2017 at 3:26 PM, Aarthi Roopnarain <AarthiR@miway.co.za> wrote:
Good day Nobu
This is a reminder of yesterdays managers meeting. The final decisions was to reject 90% of claims made by black people as from 1 August 2017.
They are an easy target, its also a great opportunity to save money and also punish these black baboons.
Kind regards,
Aarthi Roopnarain
Claims Assessor
t: 011 990 0676 | f: 011 990 0676 | e: AarthiR@miway.co.za
MiWay .co.za
#insurancefreedom
MiWay Emergency Alert
Your silence is our signal.
Ts & Cs Apply
MiWay Insurance Ltd. 48 Sterling Road, Samrand Business Park, Kosmosdal Ext 12, 0157, Gauteng
Reg No: 2007/026289/06. An Authorised Financial Services Provider (Licence No: 33970)
Board of directors. View our email disclaimer, alternatively send a blank e-mail to disclaimer@miway.co.za
Help the environment - please don't print this email unless you really need to!


mimecast
Administration
Search Mimecaster Central
Dashboard
Policies
Gateway › Policies
Go Back
Save
Save and Exit
View Plain Text
Hide Borders
Select Layout
Edit HTML
Properties
Description
MiWay_Disclaimer_Banner
Unique Identification Text
Short Code
miway
Survey
Create missing HTML Body
Link Images (Embedded by Default)
HTML VIEW
Mimecast Stationery,
This example text is used to illustrate the latest reply in an email message that has been enhanced with Mimecast Stationery. Layouts provide a convenient mechanism for arranging email text and associated graphics.
Regards
Mimecast Development Team
Enjoying your winter snuggles?
Buy your insurance online and get cash rewards - without leaving the comfort of your bed.
Click here to find out more
Mimecast Stationery,
This example text is used to illustrate the entire email body, excluding the most recent reply, in an email message that has been enhanced with Mimecast Stationery. Layouts provide a convenient mechanism for arranging email text and associated graphics.
Regards


mimecast
Administration
Dashboard
Policies
Gateway > Policies
Go Back
Save
Save and Exit
Options
Policy Narrative
Default Stationery Assignment Policy
Select Stationery
MiWay_Disclaimer_Banner
Lookup
Preview
Emails From
Addresses Based On
The Return Address (Email Envelope From)
Applies From
Email Domain
Specifically
miway.co.za
Emails To
Applies To
External Addresses
Specifically
Applies to all External Recipients
Validity
Enable / Disable
Enable
Set policy as perpetual
Always On
Date Range
All Time
Policy Override
Bi Directional
Source IP Ranges (n.n.n.n/x)

ANNEXURE D

Configuration for enabling litigation on hold as per below,

```
#########################################################################

###            Exchange Online                          ###

### Here you create a session for Exchange Online and connect to it   ###

#########################################################################


$exchangeSession = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri "https://outlook.office365.com/powershell-liveid/" -
Credential $Tenantcredentials -Authentication "Basic" -AllowRedirection


Import-PSSession $exchangeSession ñAllowClobber



#########################################################################

#####                 Add litigationHold                      ###

#########################################################################
Get-Mailbox -ResultSize unlimited | Where {$_.LitigationHoldEnabled -match "False"} | ForEach-Object {

$Identity = $_.alias; Set-Mailbox -Identity $Identity -LitigationHoldEnabled $True }
```

Aarthi Roopnarain
Mon 03-27, 03:26 PM
'djmondlim@gmail.com'; INVDOCS

You forwarded this message on 2017-07-20 01:53 PM

CONSENT LETTER.pdf
95 KB

Download Save to OneDrive - MiWay

Good day Mondli,

As per our discussion, please sign and send back to me so that I can request the report on your behalf.

Kind regards,

Aarthi Roopnarain

Claims Assessor

t: 011 990 0676 | f: 011 990 0676 | e: AarthiR@miway.co.za

MiWay .co.za

#insurancefreedom