

2018

SABRIC ANNUAL CRIME STATS 2018

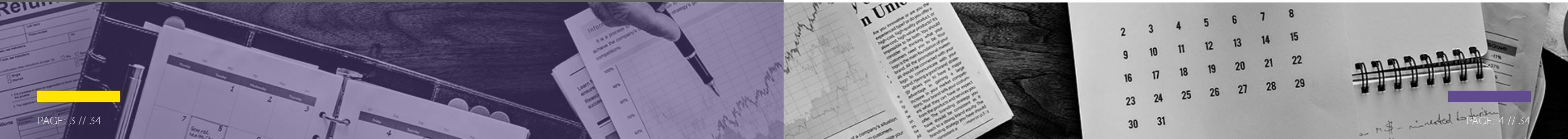
VIOLENT CRIME | DIGITAL CRIME | CARD FRAUD



Table of Contents

| | |
|-------------------------------------|-----------|
| Executive Summary | 05 |
| Qualification of Information | 06 |
| Violent Crime | 07 |
| Associated Robbery | 07 |
| ATM Attacks | 09 |
| Burglary | 11 |
| Bank Robbery | 13 |
| Cash in Transit Robbery | 15 |
| Digital Crime | 17 |
| Digital Banking Fraud | 17 |
| Banking Apps | 18 |
| Online Banking | 20 |
| Mobile Banking (USSD) | 22 |

| | |
|--|-----------|
| Card Fraud | 25 |
| Debit & Credit Card Losses: All Fraud Types, All Countries | 25 |
| Debit & Credit Card Losses: All Fraud Types, South Africa Only | 25 |
| South Africa vs Abroad | 26 |
| Fraud Types | 27 |
| Card Not Present | 28 |
| Lost & Stolen | 29 |
| Counterfeit | 30 |
| Card Fraud: ATM vs POS | 31 |
| International Perspective: SA Issued Credit Cards | 31 |
| International Perspective: SA Issued Debit Cards | 32 |
| Find us Online | 33 |



Executive Summary

Syndicates are opportunistic and continually adjust their tactics to take advantage of any opportunities to get their hands onto bank client's cash, albeit via a cash robbery, stolen card data or solicited confidential information.



SABRIC's unique repository for banking industry crime data enables analytical capabilities to unpack and understand banking fraud trends. Using multiple point-to-point connections between users and data suppliers, we can collate data, extract information and reveal the insights that you will be privy to in this publication.



In the violent crime space, our work in supporting our Cash-in-Transit (CIT) company members as well as law enforcement has helped reduce the scourge of violent attacks, which reached new levels in 2018. There were many successes which would not have been possible without collaborative and dedicated efforts with our partners.



With regards to cybercrime, history has shown that innovation is followed by disruption. The evolution of banking has seen the emergence of digital platforms for bank clients to self-service without ever having to set foot in a bank branch. New and innovative banking channels also create new opportunities for criminals to exploit unsuspecting banking clients using social engineering.



As with cybercrime, card fraud has seen a dramatic increase as criminals find new ways of accessing client card data, mostly through social engineering. It is therefore imperative that bank customers become aware that they need to be extra careful about where and how they use their bank cards and bank card information.

The resulting trends derived from SABRIC's banking crime statistics don't only enable our banks to deploy effective risk mitigation strategies, they also make the public aware of how criminals are targeting them. If we want to beat bank-related crime, we unfortunately must accept that as individuals, we also have the responsibility to protect our money and hopefully in doing so, will help to spread the word to others. We certainly have a moral duty to help each other and contribute to restoring confidence in our communities and in turn our country.



Qualification of Information



The information utilised in this publication was provided by SABRIC members. The statistics used in the report cover the period from **01 January to 31 December 2018**.

The information used was as follows:

- For the comparative analysis, the above-mentioned period was compared to **2017**.
- All calculations are based on the date that the incident or fraudulent transaction occurred.
- All violent crime losses mentioned in this publication refer to cash that was robbed or stolen and excludes cash that was recovered as well as other damages incurred.
- All fraud losses mentioned in this publication refer to gross fraud losses.
- Loss figures are rounded to the nearest **R1 million**, unless otherwise stated and therefore the sum of the separate losses (for example per loss category/fraud types) may differ from the rounded loss reflected.



Violent Crime

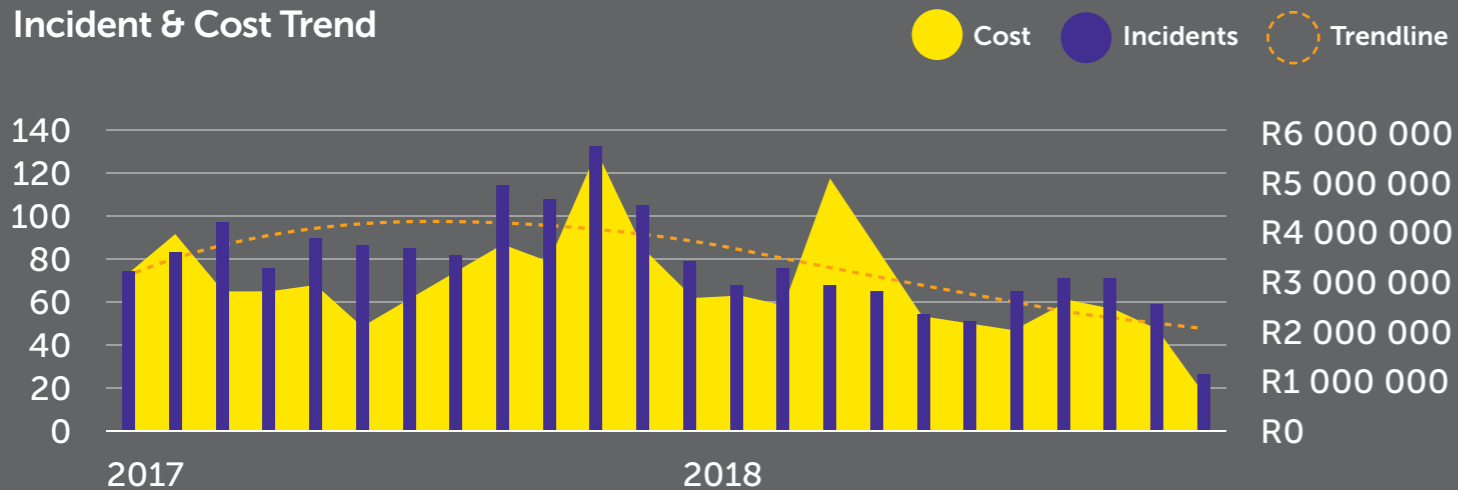
Associated Robbery

- Associated Robbery at the branch after making a withdrawal is the most prominent modus operandi (MO).
- Associated Robbery at the branch before making a deposit is the second most prominent MO.
- Incidents at the ATM after making a withdrawal and before making a deposit has shown an increase and is concerning.

-33% decrease associated robbery incidents from 2017 - 2018

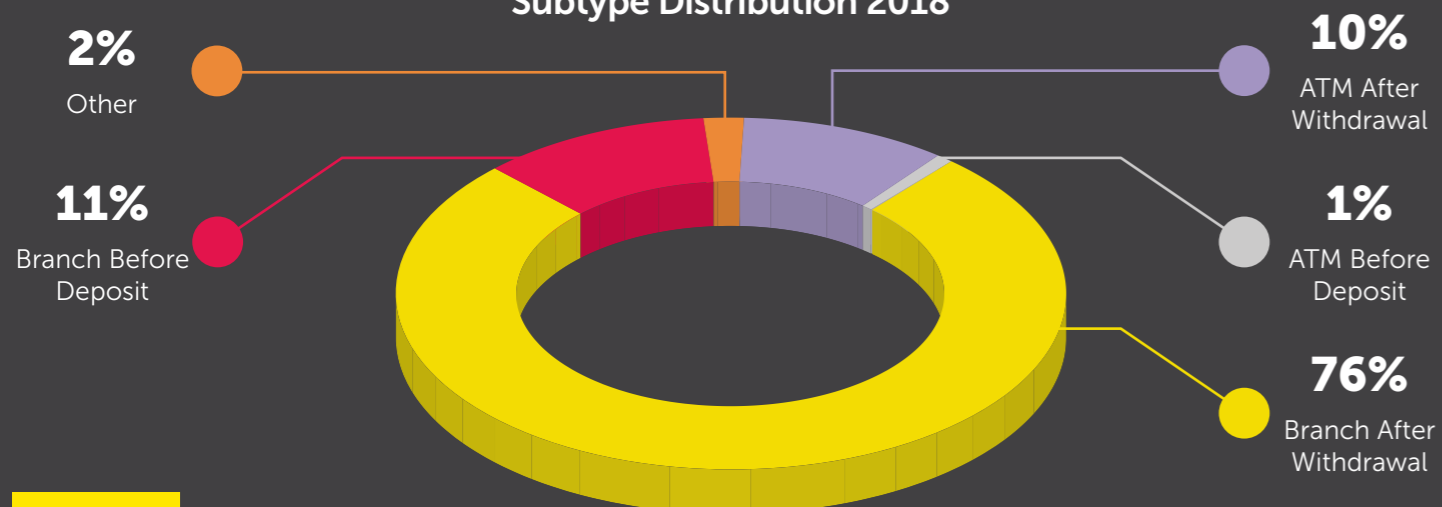
-22% decrease associated robbery losses from 2017 - 2018

Incident & Cost Trend



The decline noted during both December periods could be attributed to law enforcement festive season operations and crime awareness media coverage generated by the banking industry.

Subtype Distribution 2018



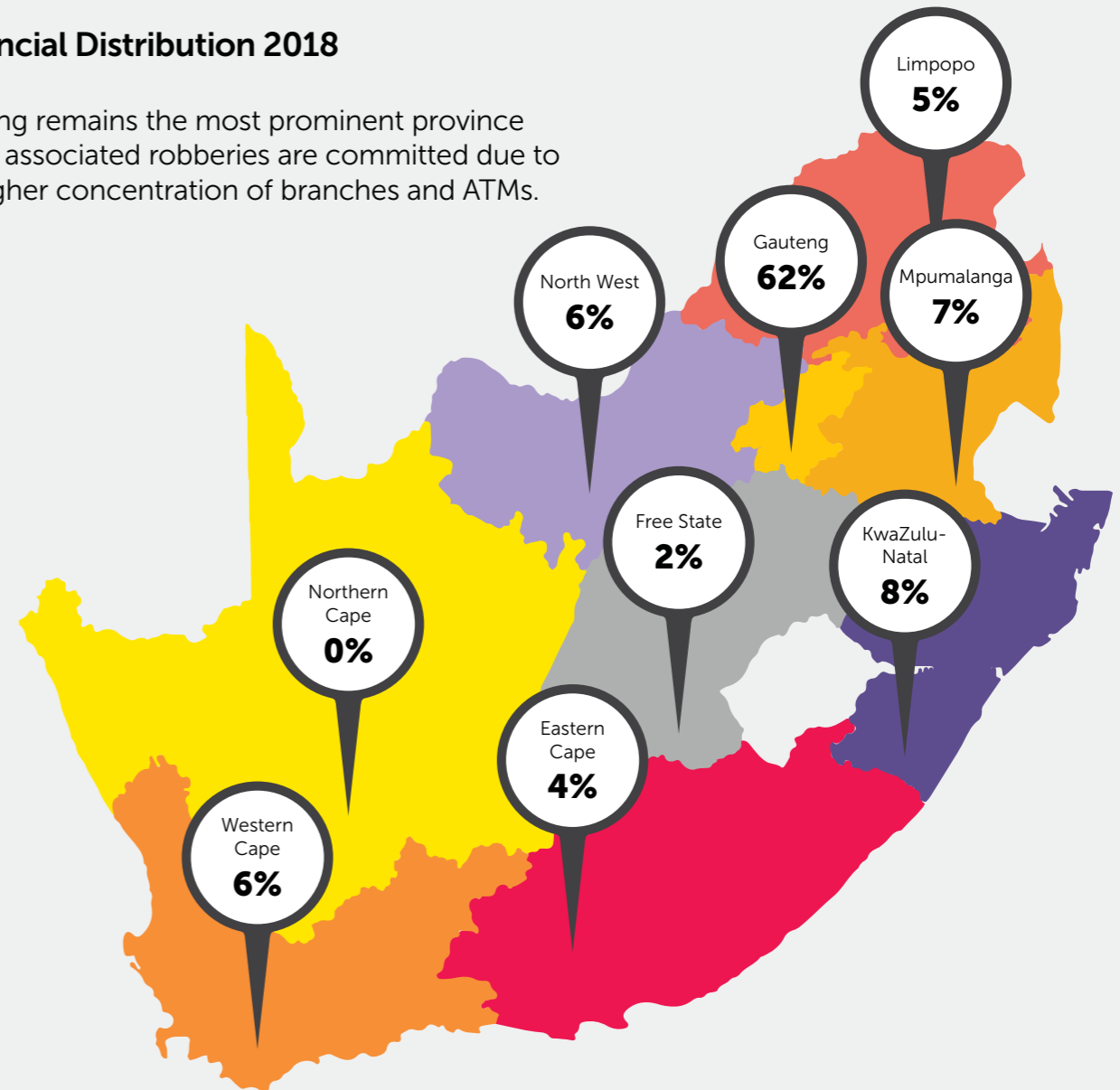
Although offenders use several modi operandi to rob clients, the most prominent one remains where offenders follow a victim and rob them of cash which they have withdrawn at a bank branch en route to their residence or to their business premises. **2018** saw incidents of associated robbery after withdrawal at an ATM increase by **7%**, while related cash losses decreased by **3%**. This could be due to the belief by perpetrators that clients withdrawing cash from ATM machines are easier targets, despite the cash reward being lower than clients withdrawing cash inside the branch.

A variation of the follow home modus operandi is where the victim is lured into motor vehicle under the pretext of being offered a lift.

In some incidents perpetrators use a minibus and pretend to be the driver. The victim is then convinced to make use of the taxi, driven to a secluded location and robbed of their cash. In many cases the victim is also robbed of their bank card and forced to divulge their PIN code.

Provincial Distribution 2018

Gauteng remains the most prominent province where associated robberies are committed due to the higher concentration of branches and ATMs.



ATM Attacks

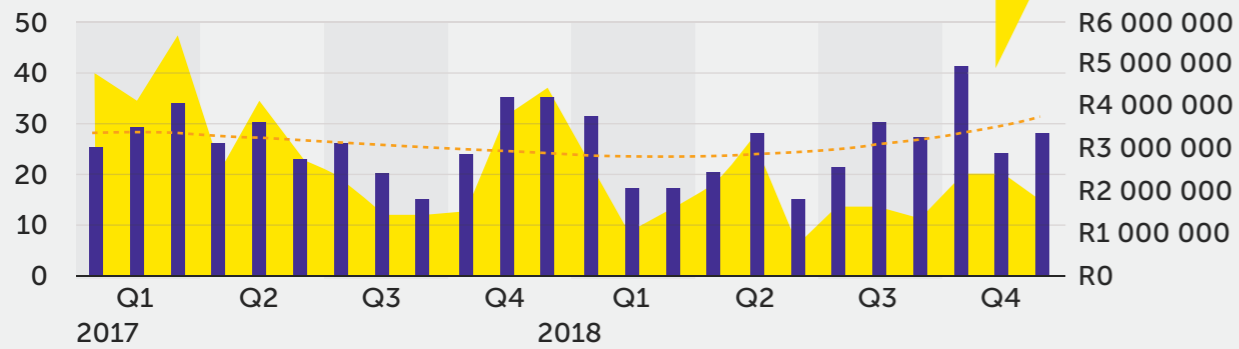


-7% decrease in ATM attack incidents from 2017 to 2018.

-42% decrease in cash losses from 2017 to 2018.

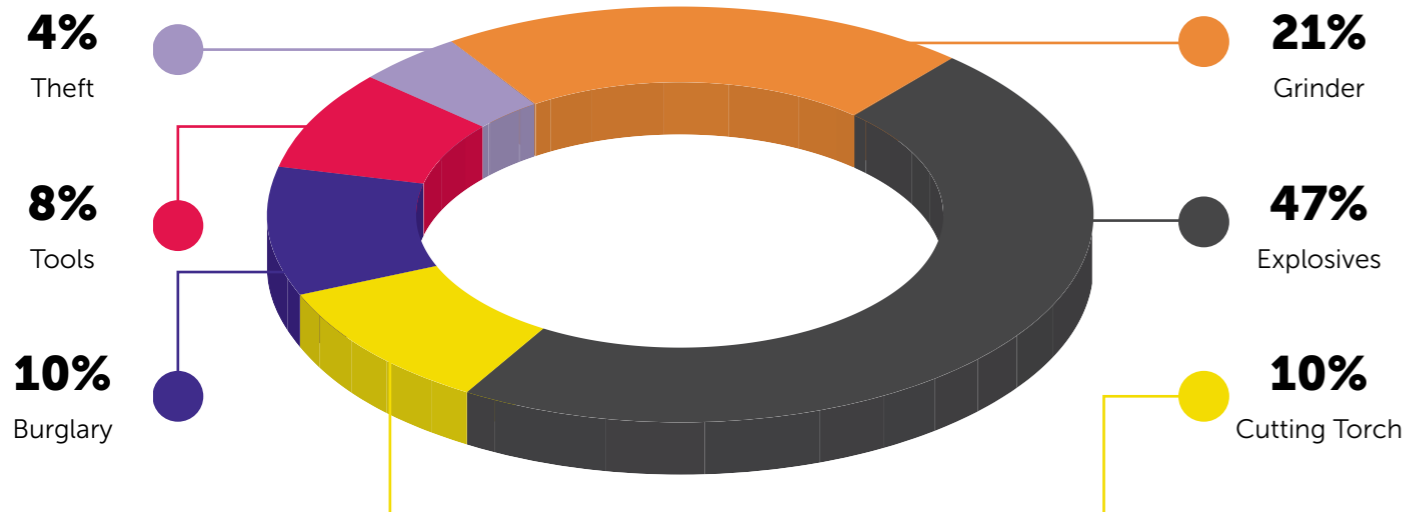
Incident & Cost Trend

● Cost ● Incidents ○ Trendline



ATM attacks using explosives showed a steady increase in Q3 & Q4 of 2018

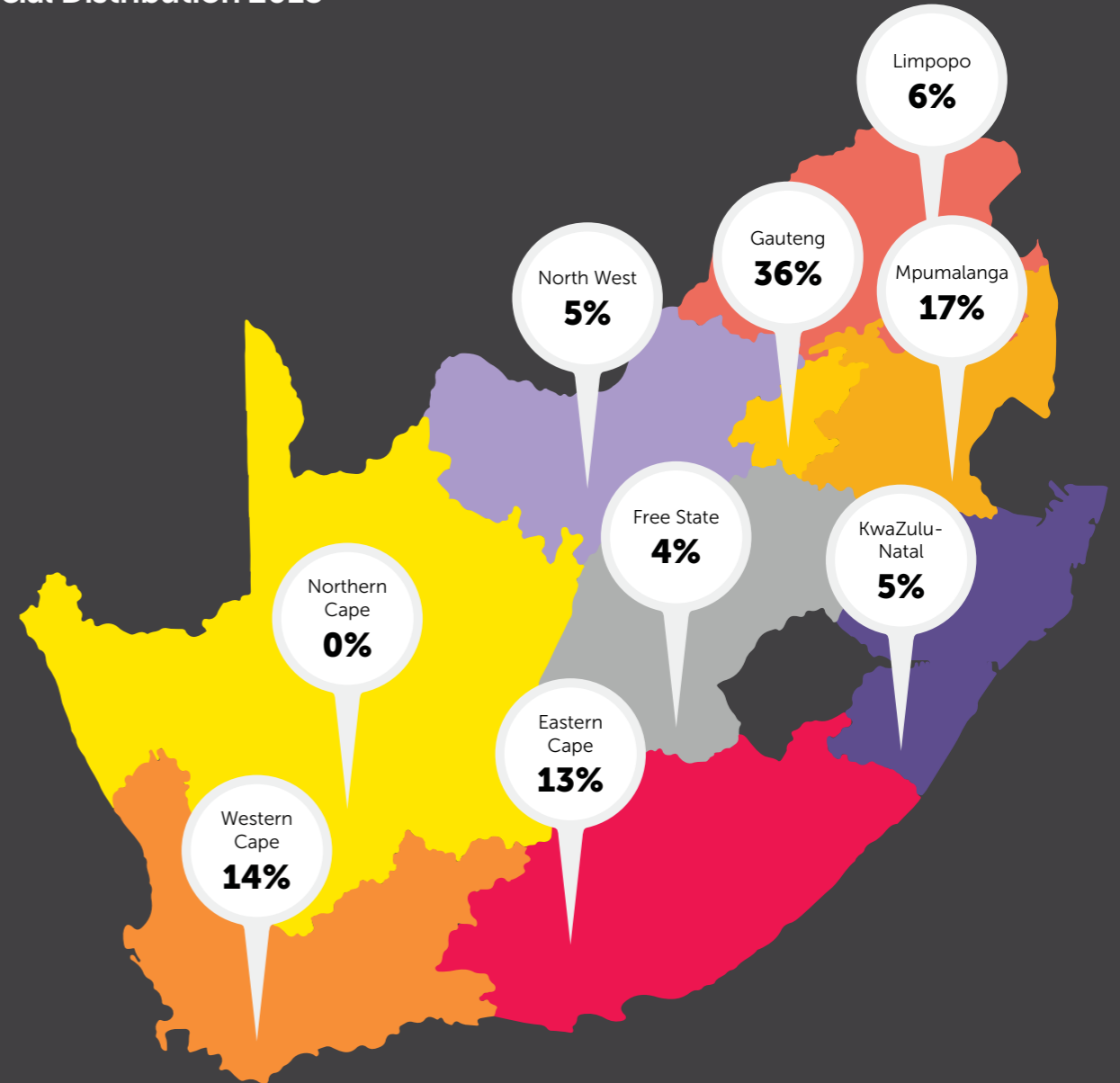
Subtype Distribution - 2018



ATM attack incidents using explosives increased by **26%** during **2018** when compared to **2017** however losses decreased by **15%** for the same period. Although there was an increase in recorded attacks during **2018**, most (**70%**) of them were unsuccessful and may have been perpetrated by inexperienced criminals. In most

reported incidents, the fascia of the ATM was damaged but even in cases where there was severe damage, the safe was not breached. The theft of ATMs from retail stores re-emerged in the Eastern Cape in **2018** where perpetrators physically removed the lobby-type ATM and loaded it onto a light duty vehicle.

Provincial Distribution 2018



Gauteng reported the most incidents (**36%**) followed by Mpumalanga (**17%**), the Western Cape (**14%**) and the Eastern Cape (**13%**).



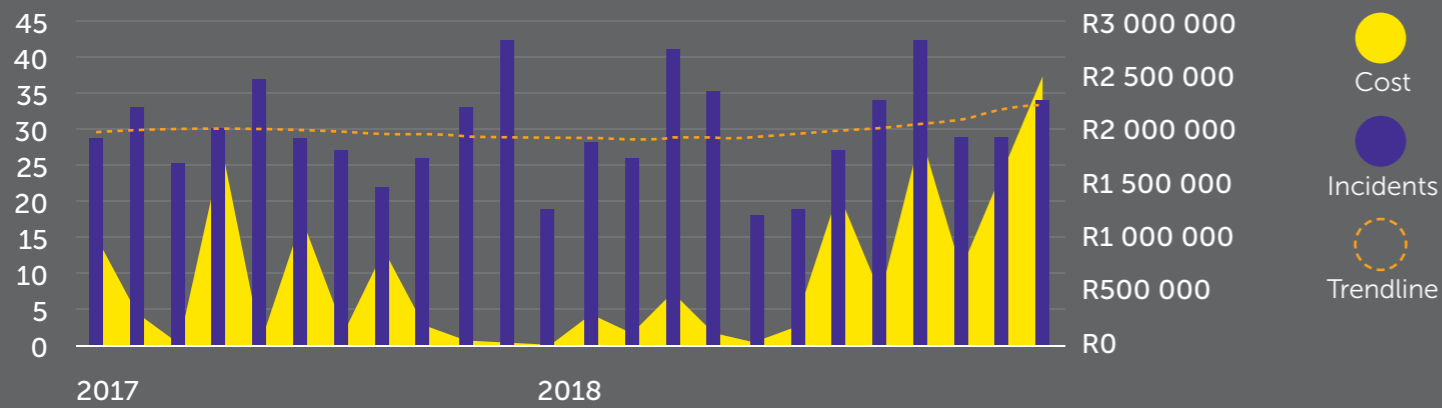
Burglary



2018 saw a **+3%** increase in burglary incidents and a **+75%** increase in losses compared to 2017.

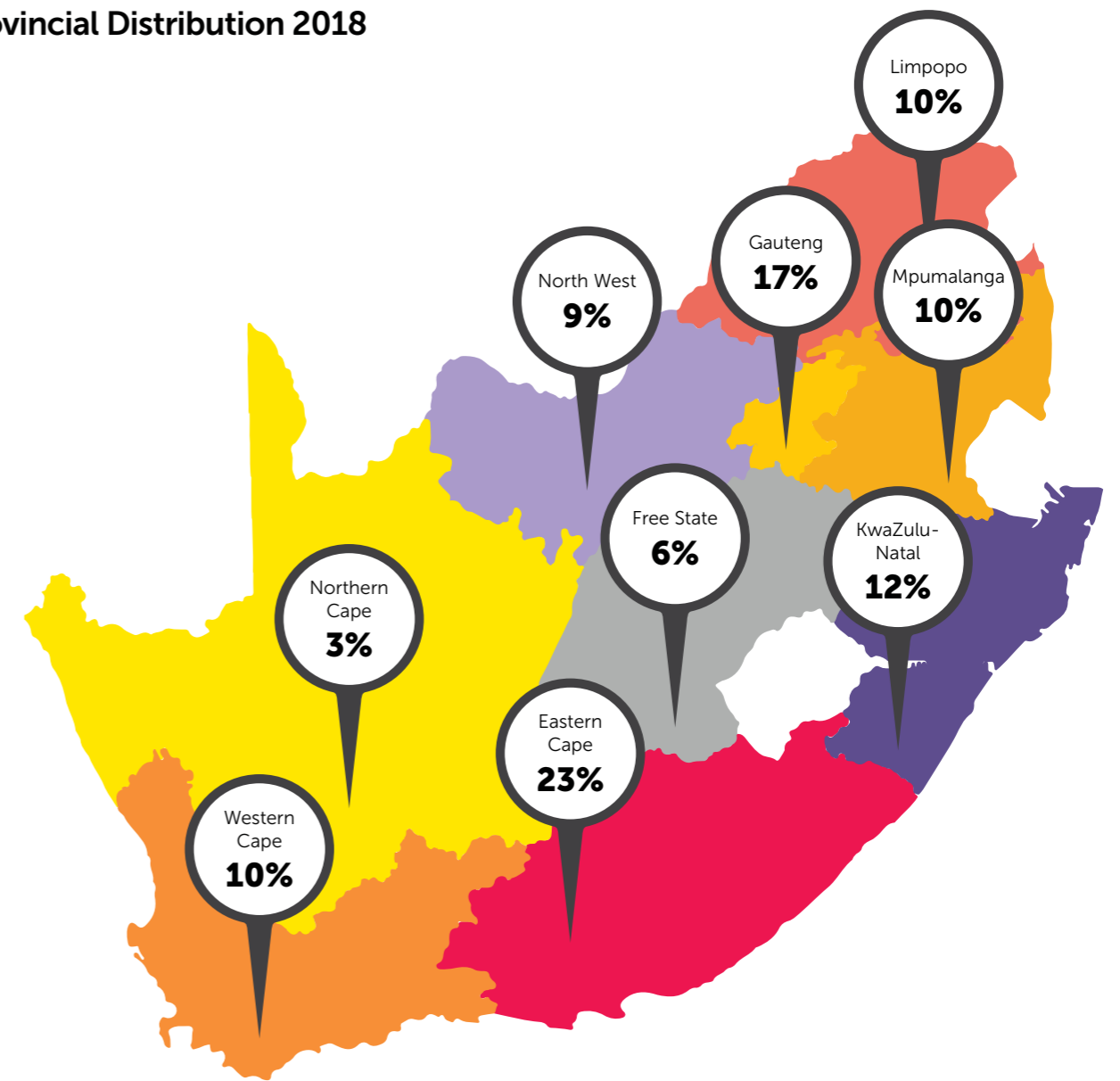
Subtype 'Burglary Cash' incidents increased by **+29%** from 2017 - 2018 with a **+76%** increase in losses for the same period.

Incident & Cost Trend

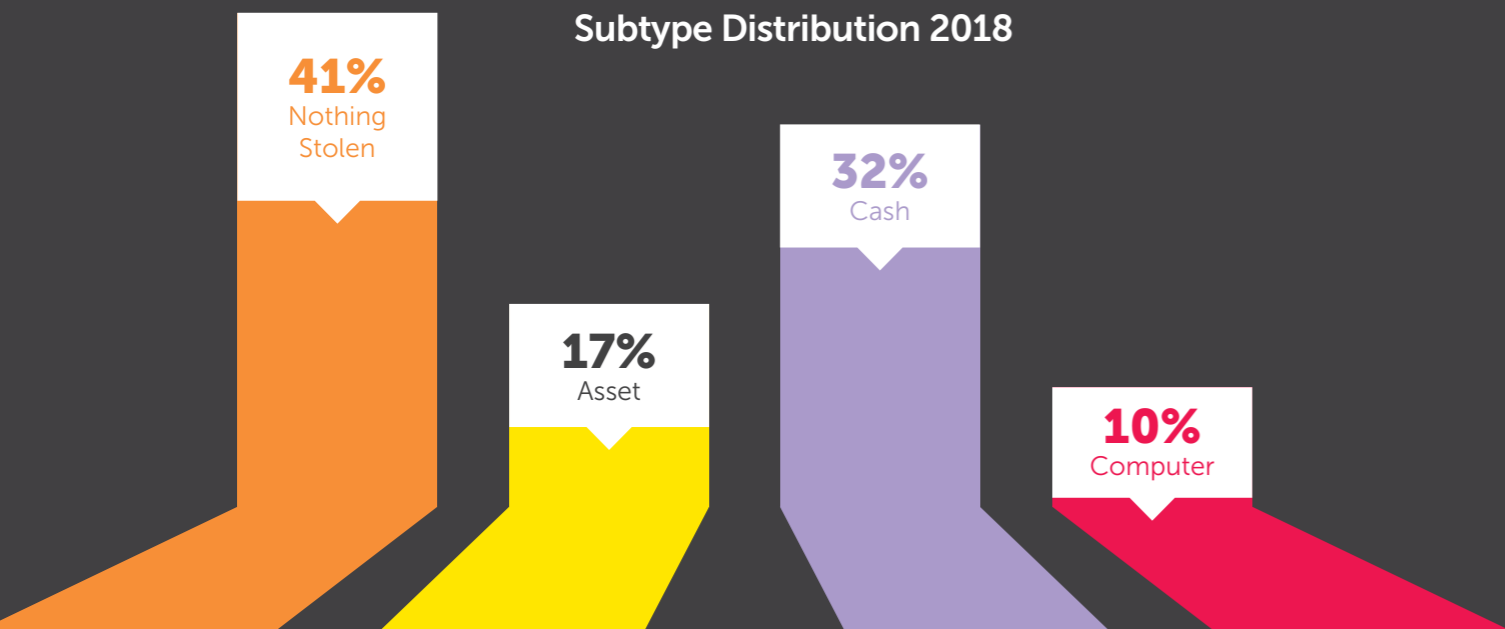


2018 saw an overall upward trend for burglary. Of concern is the increase in cash losses that were reported from the second half of 2018.

Provincial Distribution 2018



Subtype Distribution 2018

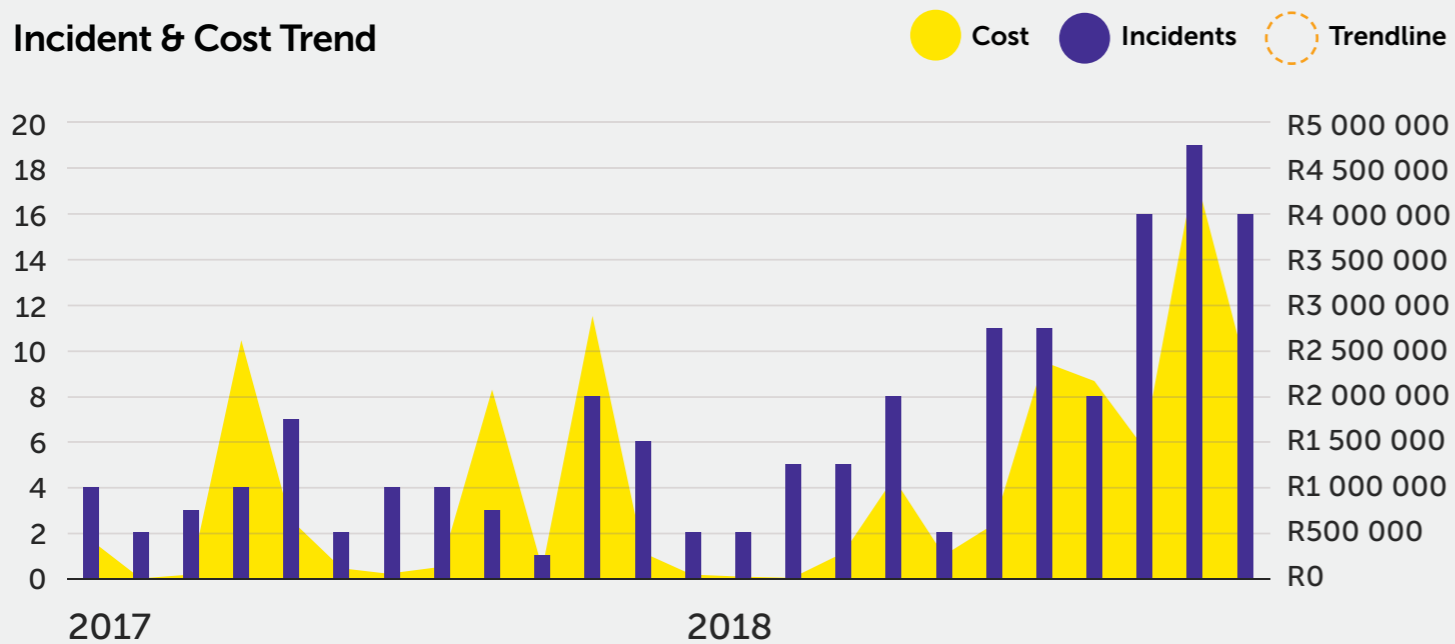


Bank Robbery

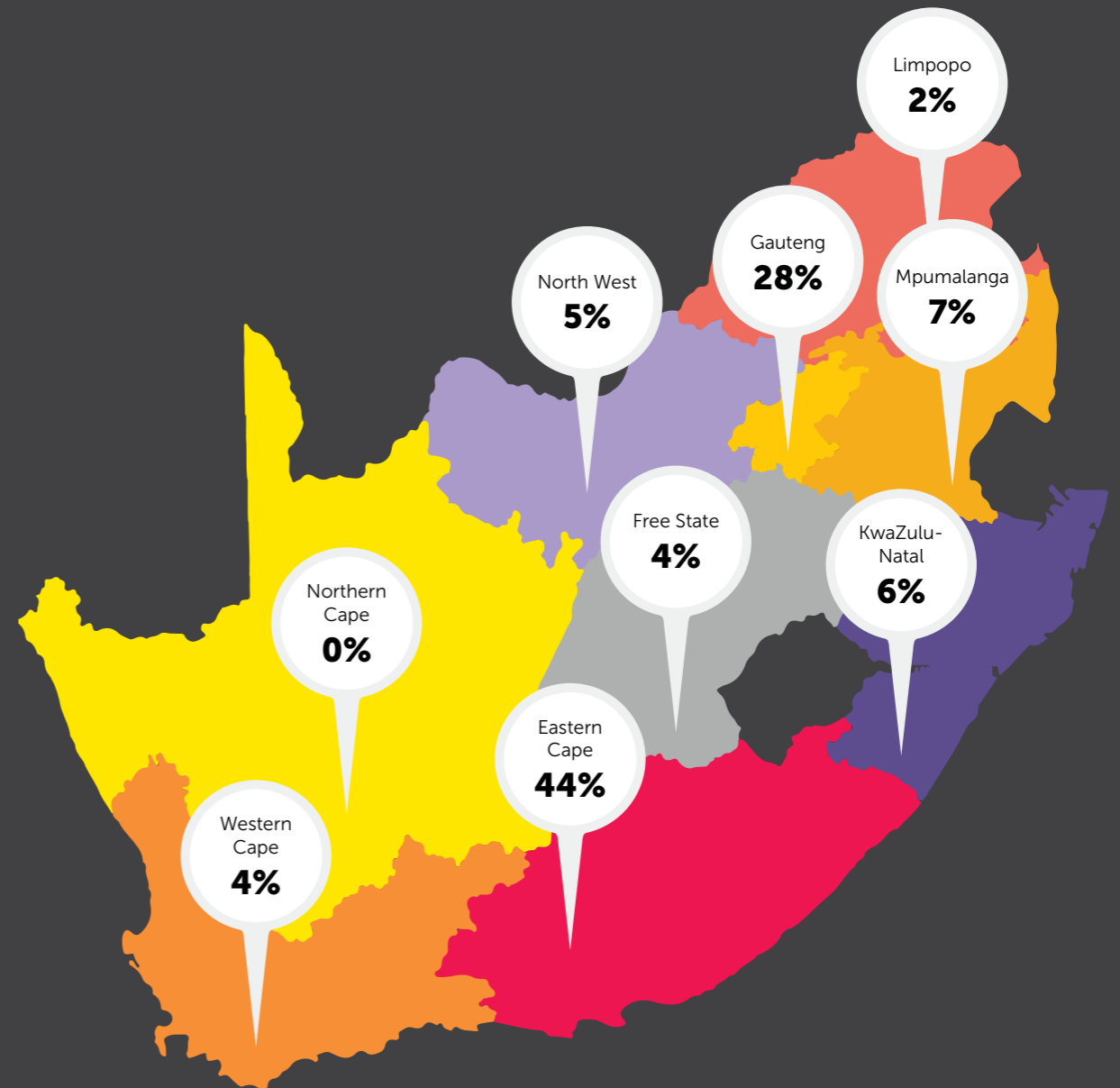


From **2017 - 2018** there was an increase in bank robbery incidents of more than **100%** with a **+59%** increase in losses.

Incident & Cost Trend



Provincial Distribution 2018



Cash in Transit Robbery



Cash in transit (CIT) robberies and their associated cash losses reflect a downward trend.

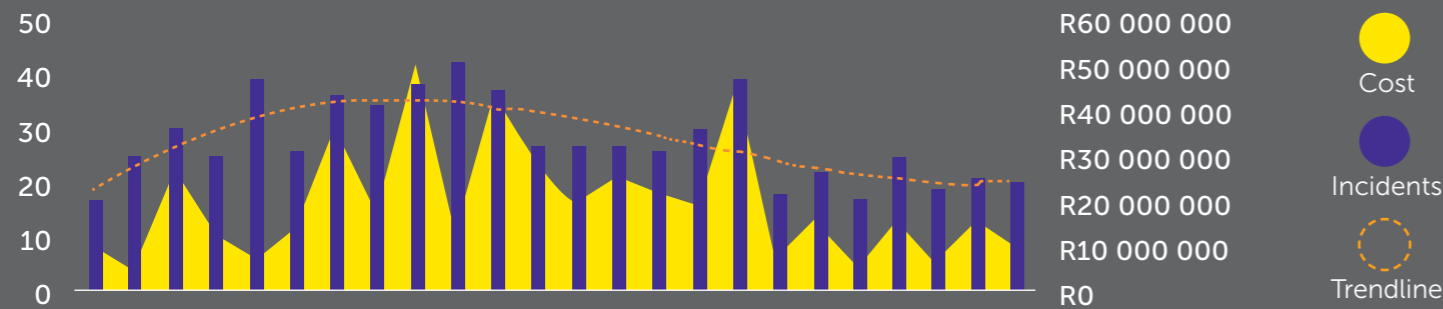
CIT incidents decreased by **-22%** from **2017 (376 incidents)** to **2018 (292 incidents)**.

Cash losses also showed a decrease of **-22%** for the same period.

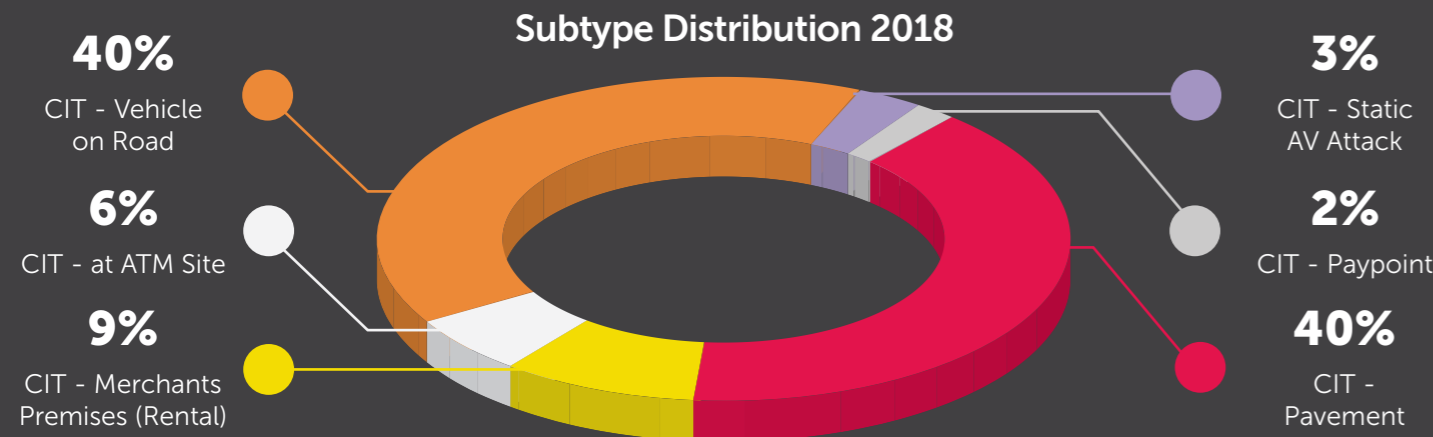
The following CIT crime subtypes contributed primarily to the overall incidents and cash losses suffered by the CIT industry from **2017 to 2018**:

- Vehicle on Road (VOR) attack incidents increased by **16%** while cash losses decreased by **17%**.
- Cross Pavement attack incidents decreased by **36%** while cash losses decreased by **31%**.

Incident & Cost Trend

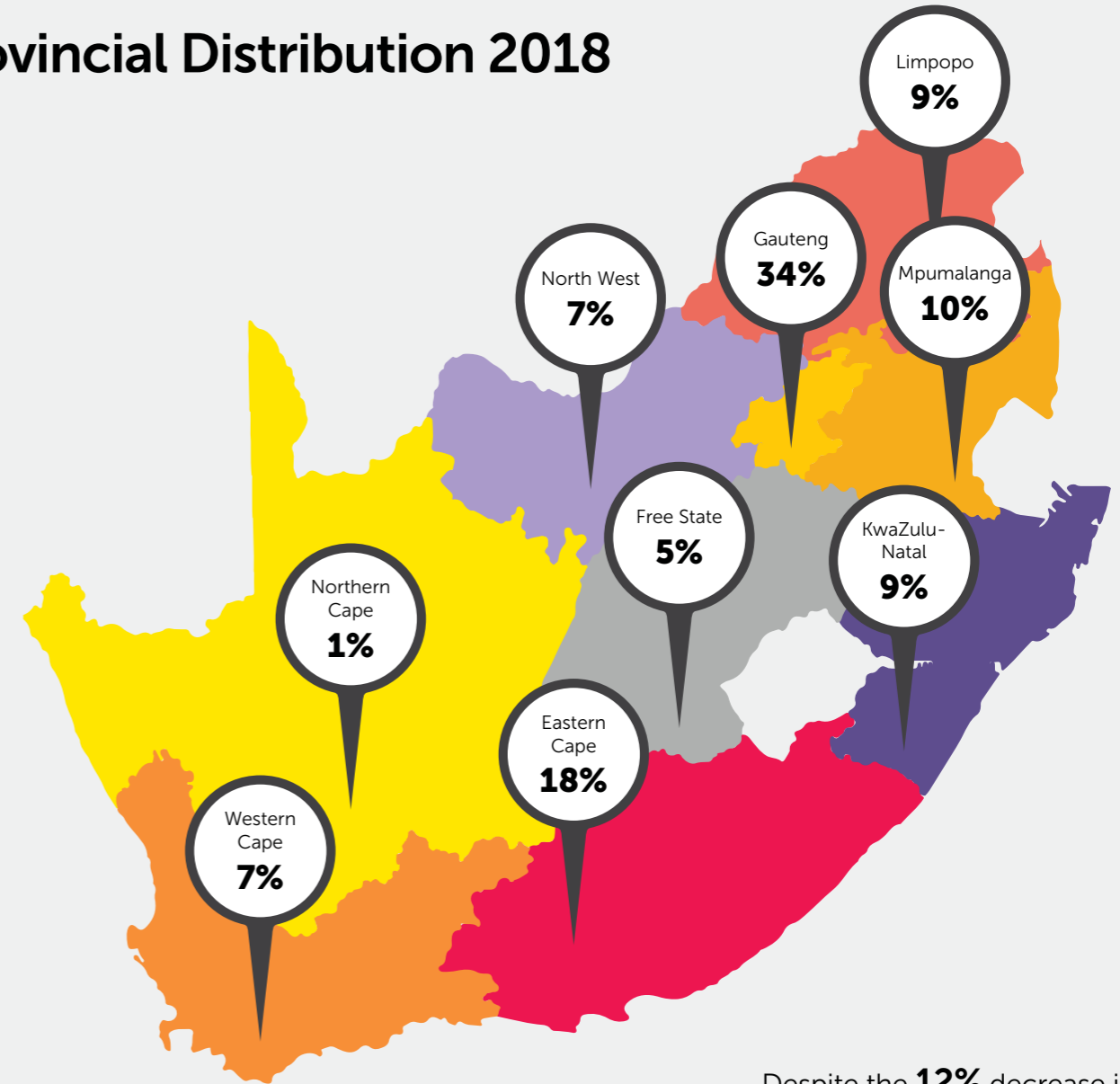


CIT incidents were prevalent in **2017** and continued in **2018**, peaking in May. After interventions by the SAPS and CIT companies, these incidents began to decline. Interventions included the SAPS led GANOLIMP a multi-party operational CIT initiative that was initiated in **May 2018** to enhance detection and investigation, prevention as well as response and intelligence gathering of CIT incidents in the provinces of Limpopo, Gauteng, North West and Mpumalanga.



During **2018** VOR incidents represented **40%** of the total incidents reported and equaled the number of Cross Pavement robberies (also at **40%**). Historically, Cross Pavement robberies were the prevalent CIT crime subtype. During **2017** VOR incidents represented **27%** of reported incidents and Cross Pavement robberies **50%**.

Provincial Distribution 2018



Despite the **12%** decrease in incidents in Gauteng from **2017** to **2018**, the province contributed to **34%** of reported CIT incidents in **2018**. In the Eastern Cape incidents increased by more than a **100%** from **2017** to **2018** and contributed to **18%** of reported incidents in **2018**.



Digital Crime

Digital Banking Fraud

Digital Banking Fraud Across All Platforms



These banking platforms enable digital banking fraud:

Banking Apps
A digital banking application downloaded from Google Play or Apple's App Store.

Online Banking
The bank specific online banking platform accessed via the World Wide Web.

Mobile Banking
USSD (Unstructured Supplementary Service Data), a Global System for Mobile (GSM) communication technology used to send text between a mobile phone and an application program in the network¹.

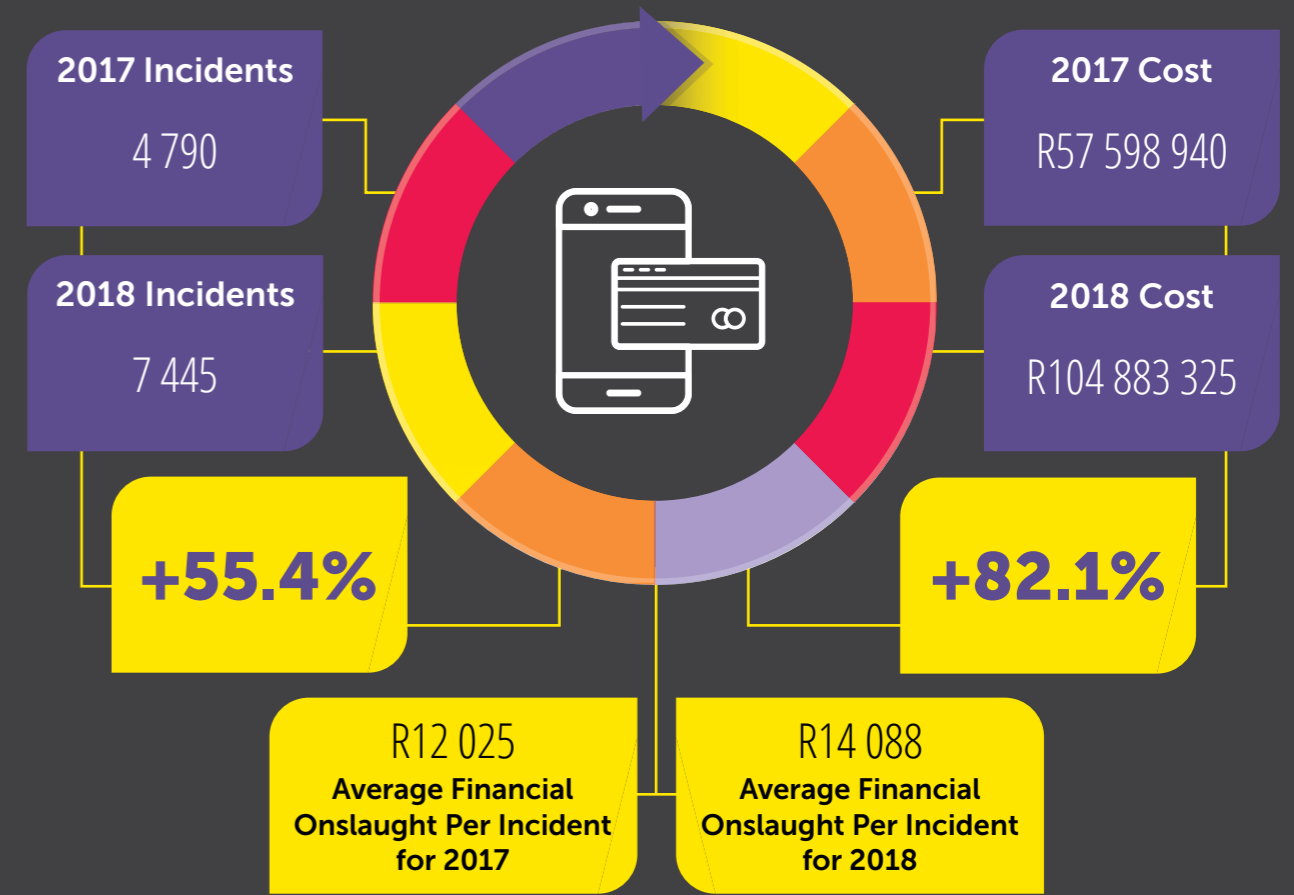
The USSD interface is a channel between a bank and a mobile network operator on which the USSD communication takes place. The technology uses a 'Global System for Mobile' (GSM) communication network to transmit information and works on basic mobile phones with black-and-white displays, feature phones and on smartphones.

USSD-based mobile banking enables bank clients to send money, check account balances, and view mini statements without the need for internet connectivity.

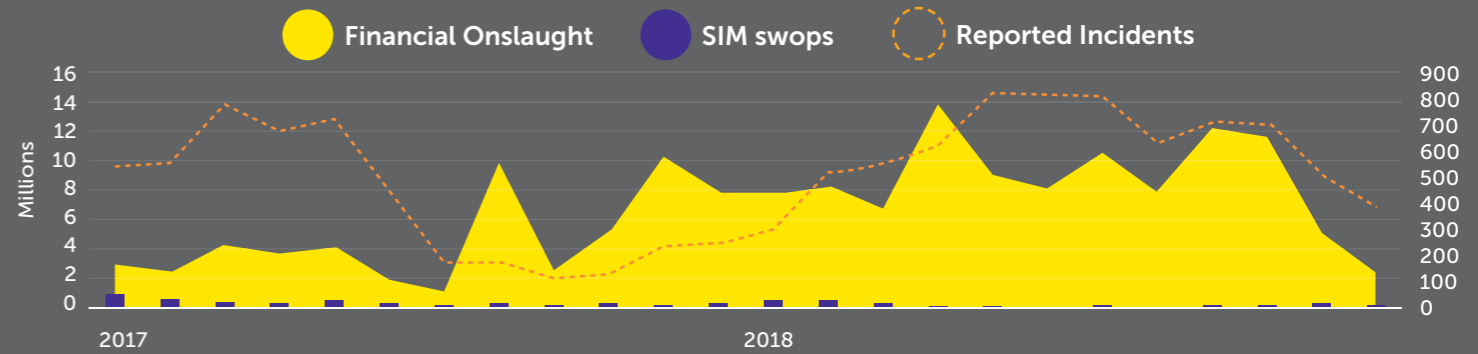
Phishing, Vishing, SMishing and Email Hacking or Business Email Compromise are the most prominent fraud types affecting the digital banking space. However, the banking industry has reported some isolated incidents where malware was used as a method of compromising a client's digital banking credentials.

¹ Please note that Wireless Internet Gateway (WIG) and Wireless Application Protocol (WAP) identified as Mobile Banking, has been discontinued by most major banks. WAP and WIG allow Internet browsing using a WAP/WIG protocol browser. WAP/WIG provides optimised (data usage and screen presentation size) interaction for mobile phones.

Banking Apps




Banking App Fraud



The increase in banking app fraud can be attributed to increased usage of this platform by bank clients. Fraudsters use Vishing to obtain transaction verification tokens also known as OTP's (One Time Passwords) and RVN's (Random Verification Number's).

The most prominent modus operandi in Banking App Fraud is Vishing. Vishing is where a fraudster **phones their victim posing as a bank official or service provider** and uses social engineering skills to manipulate them into disclosing confidential information. This information is then used to defraud the victim.

It is important to note that there have been no reports where Banking App software was compromised to commit fraud. Fraud via the Banking App is committed using social engineering tactics like **Vishing**.



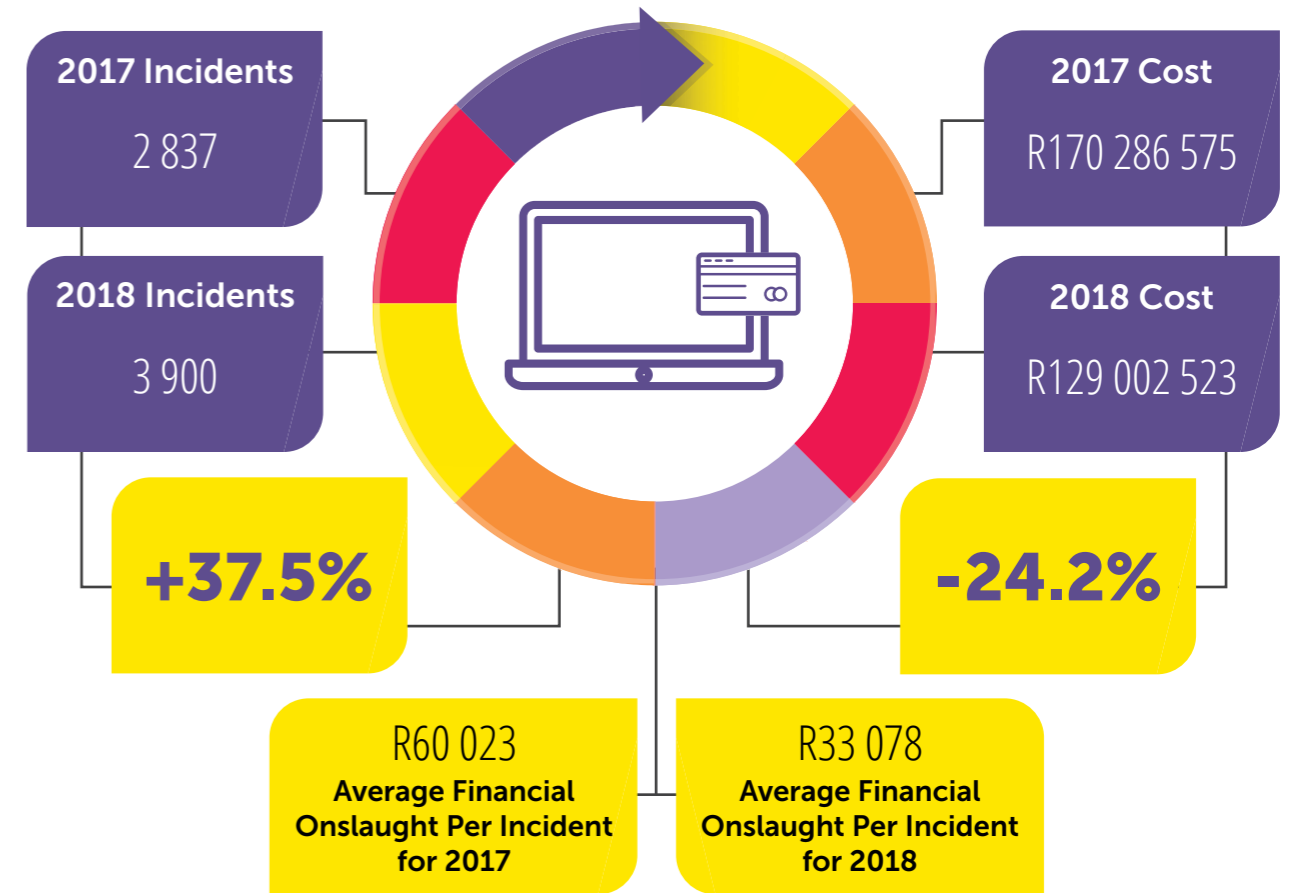
For some of these modi operandi, the criminal needs to intercept transaction verification tokens also known as OTP's and RVN's. To do this the criminal does a SIM swop via the bank clients mobile service provider. In **1.8% (137)** of Bank App fraud incidents reported to SABRIC in **2018**, SIM swops were part of the MO. This figure is a **3.2%** year on year decrease from **5.1% (243)** in **2017**.²

Number of SIM swops in the Banking App Space:

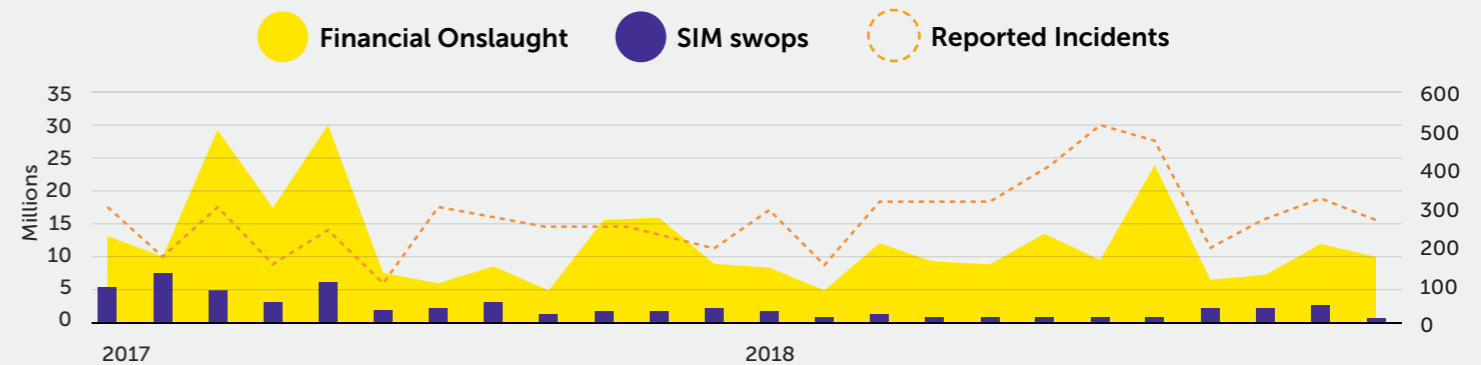


² Percentage increase is calculated by dividing the number of SIM swops done by the number of investigations. This figure is then multiplied by 100 to get the percentage.

Online Banking



Online Banking Fraud



Fraudsters use **Phishing emails** to gather client banking login credentials as this still remains the most effective way to obtain them.

From October **2018** an average of **325** new cases were reported monthly.

Phishing emails request that a user click on a link in an email which then directs them to a "spoofed" website designed to mislead them into thinking that it is their legitimate bank website, to obtain, verify or update contact details or other sensitive financial information.

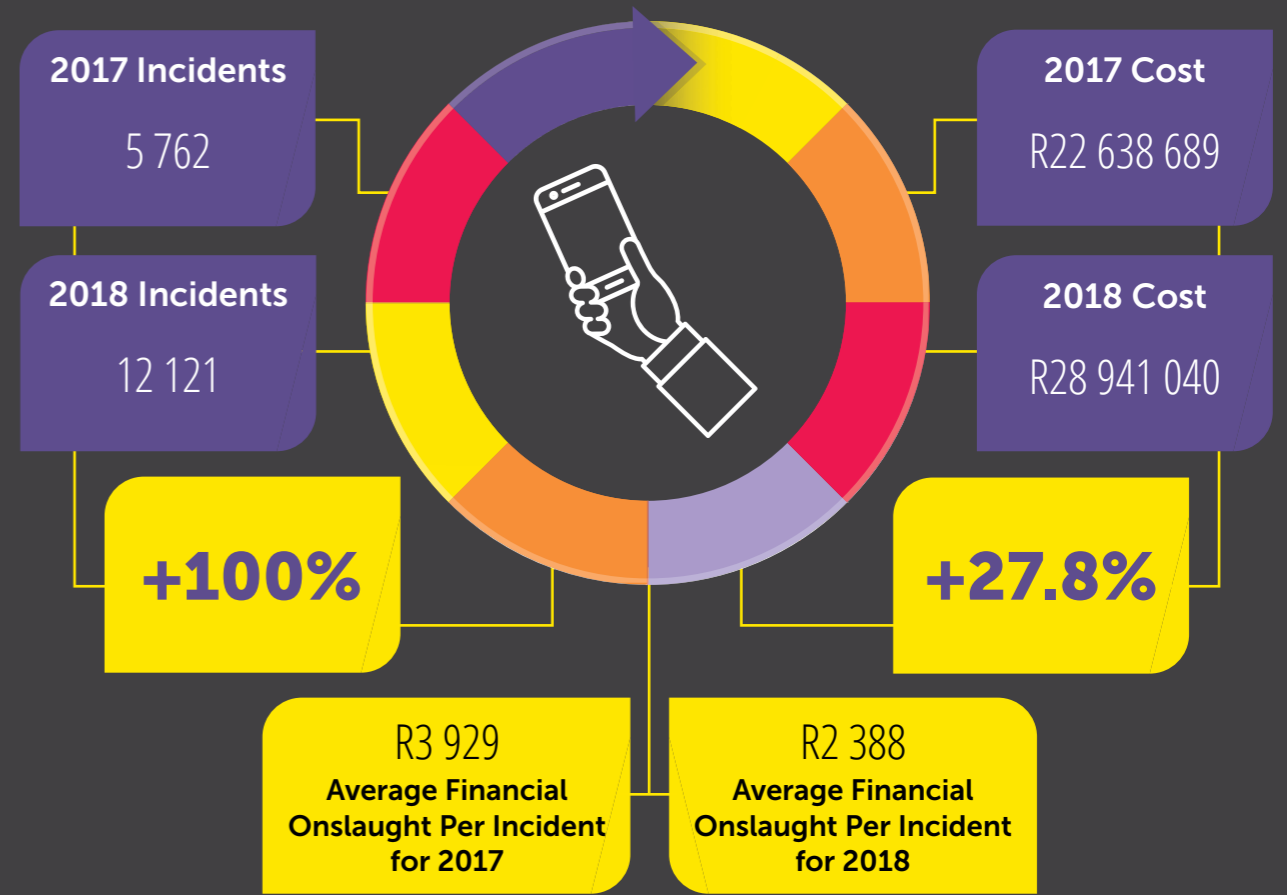


As with Bank App fraud, some of the Online Banking fraud modi operandi may also necessitate a SIM swap by the criminal to intercept transaction verification tokens (OTP's and RVN's). To do this, the criminal will need to do a SIM swap via the bank clients mobile service provider. In 5.9% (231) of the Online Banking fraud incidents reported to SABRIC in 2018, SIM swaps were part of the MO. This figure is a 18% year on year decrease from 23.9% (679) in 2017³.

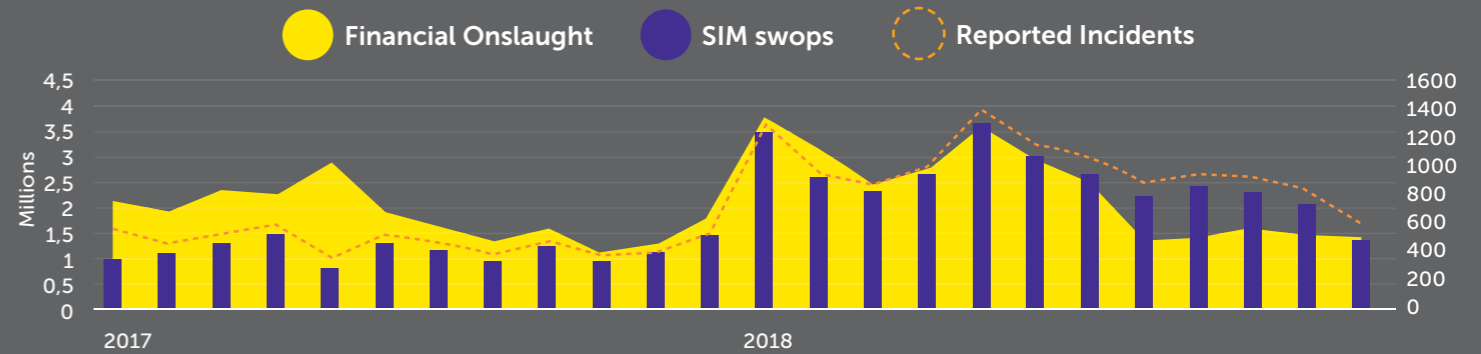
Number of SIM swaps in the Online Banking Space:



Mobile Banking (USSD)



Mobile Banking Fraud



Reported fraud on the Mobile Banking channel stabilised in the fourth quarter of 2018 after a dramatic increase from January and September 2018. This can be attributed to enhanced detection measures put in place by banks to curb fraud on this channel. October to December 2018 saw an average gross loss of R700 000 per month.

SMishing, short for "SMS phishing" is the preferred method used by fraudsters to obtain confidential information in the mobile banking fraud space. It is much the same as Phishing, except that instead of emails, text messages are sent requesting that the recipient call a number or click on a link which then misleads them into revealing their confidential information.

³Percentage increase is calculated by dividing the number of SIM swaps done by the number of investigations. This figure is then multiplied by 100 to get the percentage.



As with Bank App fraud and Online Banking fraud, some of the Mobile Banking fraud modi operandi may also necessitate a SIM swop by the criminal. To do this the criminal will need to do a SIM swop via the bank clients mobile service provider. In **91.4% (11 077)** of Mobile Banking fraud incidents reported to SABRIC in **2018**, SIM swops were part of the MO. This figure is a **5.4%** year on year increase from **86% (4 956)** in **2017**⁴.

Number of SIM swops in the Mobile Banking Space:



“We are definitely concerned about some of the increases, which clearly reflect that criminals will take every opportunity to get their hands on bank customers’ money.”

SABRIC CEO, Kalyani Pillay

⁴Percentage increase is calculated by dividing the number of SIM swops done by the number of investigations. This figure is then multiplied by 100 to get the percentage.

Card Fraud

Debit & Credit Card Losses: All Fraud Types, All Countries



+18% increase in combined gross fraud losses for credit & debit cards.

Credit card gross fraud losses **+18.4%** increase.

Debit card gross fraud losses **+17.5%** increase.

Total gross fraud losses for South African issued cards increased by **18%** from **2017 (R739.9m)** to **2018 (R873.3m)**.

Gross fraud losses on South African issued **credit cards** amounted to **R483.5m** in **2018**, an increase of **18.4%** when compared to 2017 (**R408.2m**).

Gross fraud losses on South African issued **debit cards** amounted to **R389.8m** in **2018**, a **17.5%** increase when compared to 2017 (**R331.6m**).

Debit & Credit Card Losses: All Fraud Types, South Africa Only



-2.8% decrease in combined gross fraud losses for credit & debit cards.

Credit card gross fraud losses **-4.7%** decrease.

Debit card gross fraud losses **-1.3%** decrease.

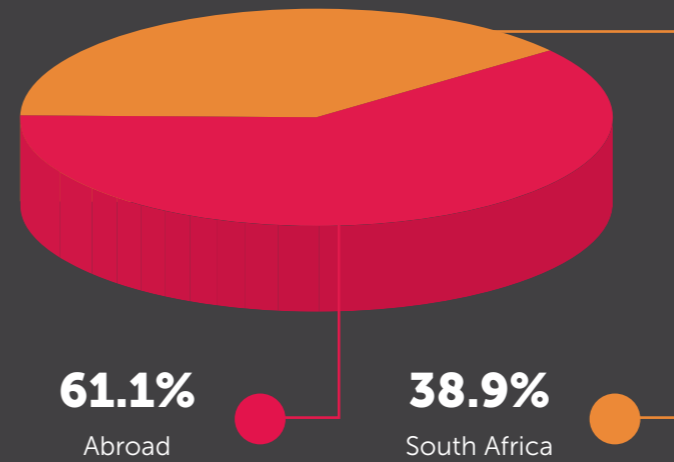
Total gross fraud losses for **2018 (R435.5m)** for South African issued cards where fraudulent transactions took place in South Africa decreased by **2.8%** when compared to **2017 (R448.3m)**.

Credit card fraud decreased by of **4.7%** when comparing **2018 (R187.9m)** to **2017 (R197.3m)**.

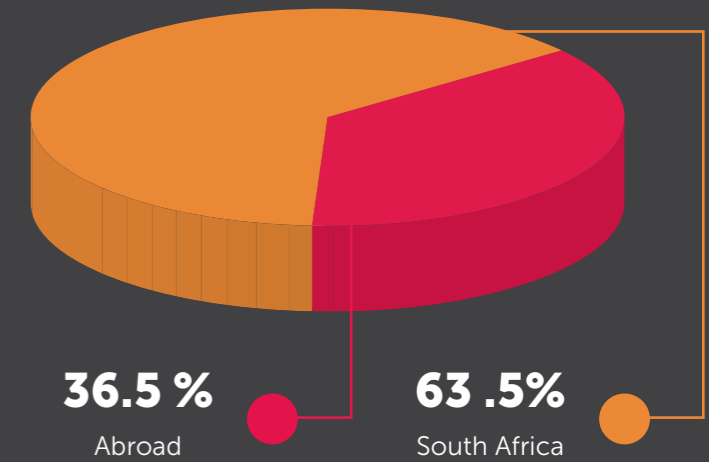
Debit card fraud decreased by **1.3%** when comparing **2018 (R247.5m)** to **2017 (R251m)**.

South Africa vs Abroad

Credit Card

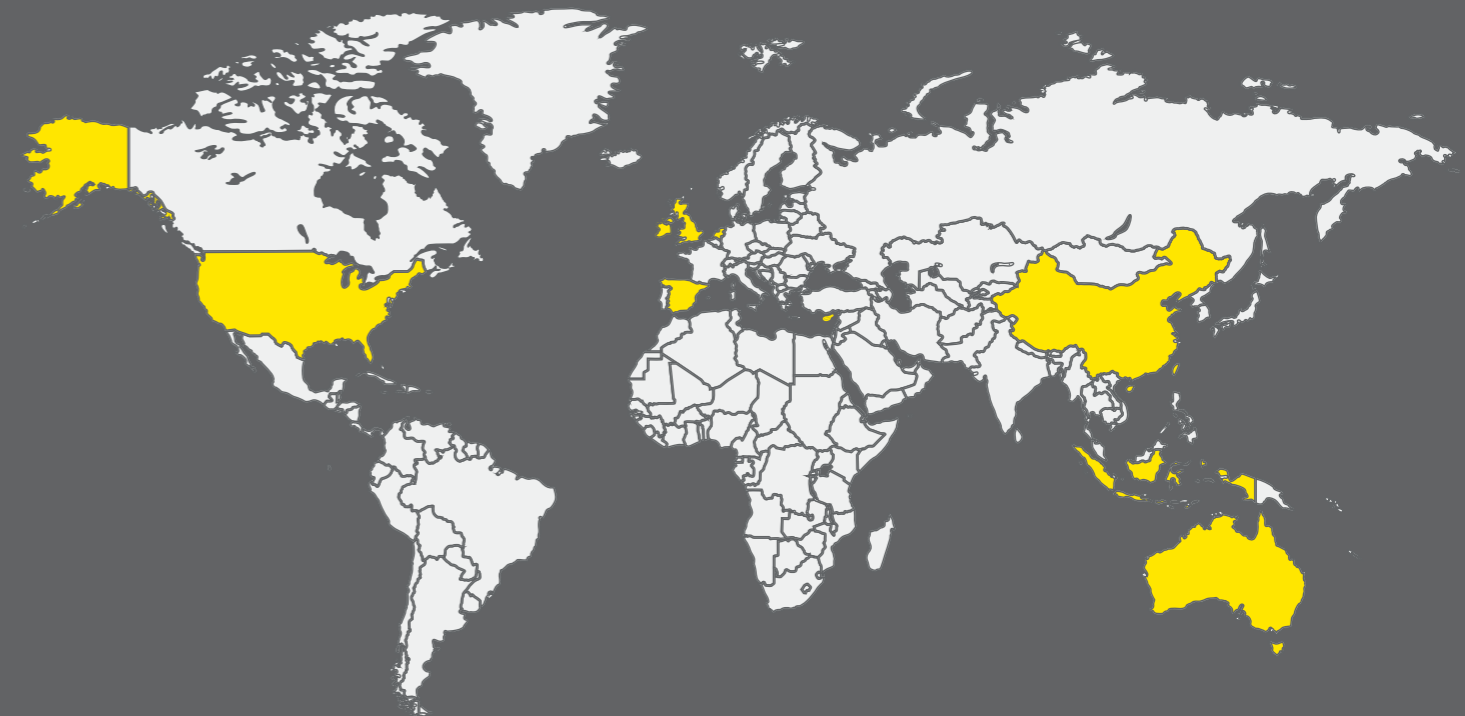


Debit Card



In **2018** **61.1%** of fraud on South African issued credit cards took place outside the borders of South Africa while **63.5%** of South African issued debit cards fraud took place in South Africa.

Below are the top countries where reported fraud took place using a South African issued debit or credit card.



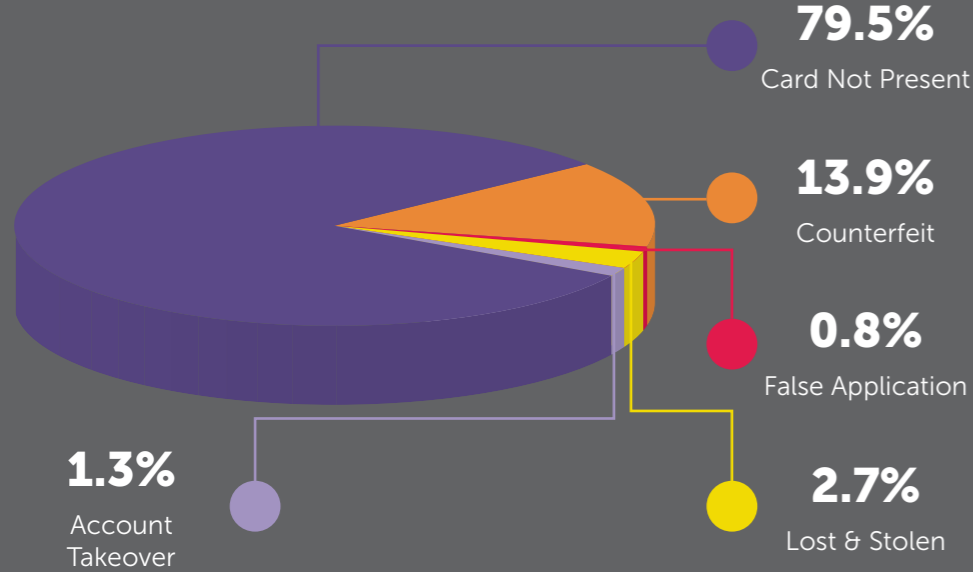
- UNITED KINGDOM
- UNITED STATES
- IRELAND
- LUXEMBOURG
- CYPRUS
- INDONESIA
- CHINA
- NETHERLANDS
- AUSTRALIA
- SPAIN



Fraud Types: All Countries

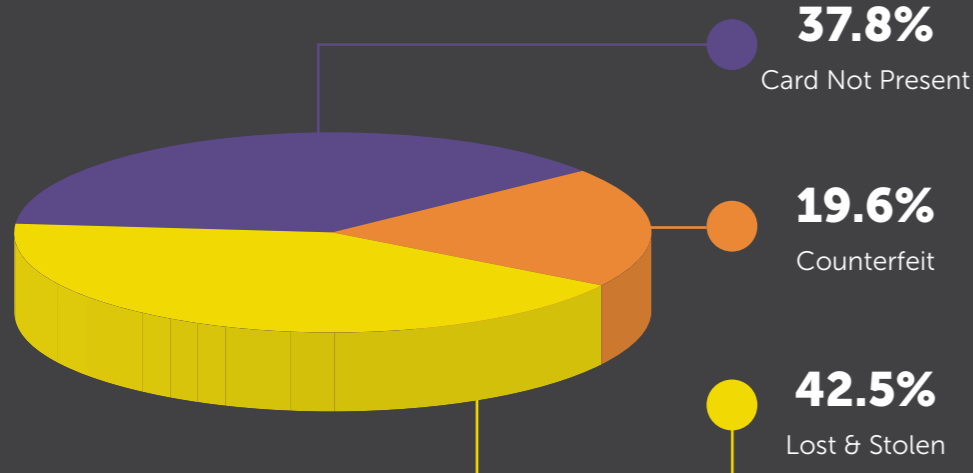
| CREDIT | RAND VALUES | DEBIT | RAND VALUES |
|---------------------|-------------|---------------------|-------------|
| Account Takeover | R7.3m | Account Takeover | R65 437 |
| Card Not Present | R384.2m | Card Not Present | R147.7m |
| Counterfeit | R66.9m | Counterfeit | R76.4m |
| False Application | R9.7m | False Application | R594 741 |
| Lost and/or Stolen | R13.1m | Lost and/or Stolen | R165.8m |
| Not Received/Issued | R1.8m | Not Received/Issued | R46 630 |

Credit Card



In **2018** Card Not Present (CNP) fraud amounted to **79.5%** of gross fraud losses on South African issued credit cards, followed by Counterfeit (**13.9%**) and Lost and/or Stolen (**2.7%**) fraud. CNP fraud increased by **28%** when compared to **2017**. There was a significant decrease of **54.9%** on Lost and/or Stolen cards when comparing **2017** to **2018**.

Debit Card



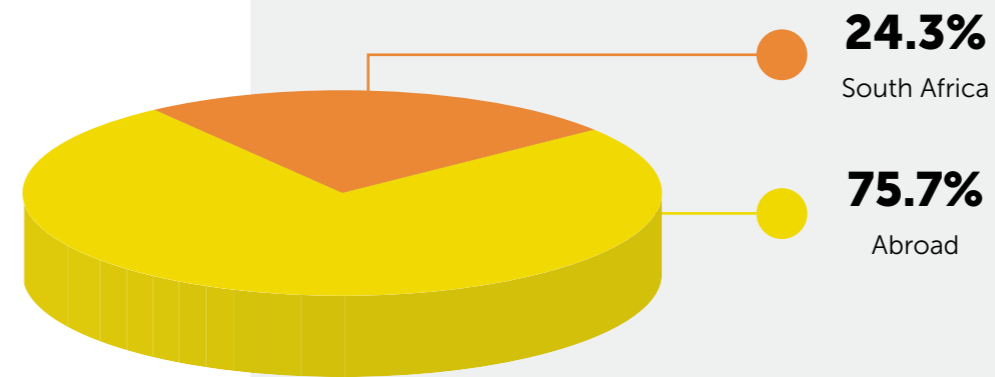
In **2018** Lost and/or Stolen debit card amounted to **42.5%**, followed by Card Not Present fraud (**37.8%**) and Counterfeit fraud (**19.6%**). Card theft or card swapping at ATMs is directly linked to Lost and/or Stolen card fraud and remains a concern. Card Not Present fraud increased by **62.3%** when 2018 was compared to 2017, this increase could be a result of more debit cards transacting online.

Card Not Present

| PRODUCT | 2017 | 2018 | Inc/Dec | CNP as % of Gross Fraud |
|---------|--------------|--------------|------------------------|-------------------------|
| Debit | R91 034 628 | R147 717 130 | +62.3% increase | 37.9% |
| Credit | R300 106 416 | R384 236 439 | +28% increase | 79.5% |

Debit

In **2018** **75.7%** of CNP debit card fraud occurred abroad.

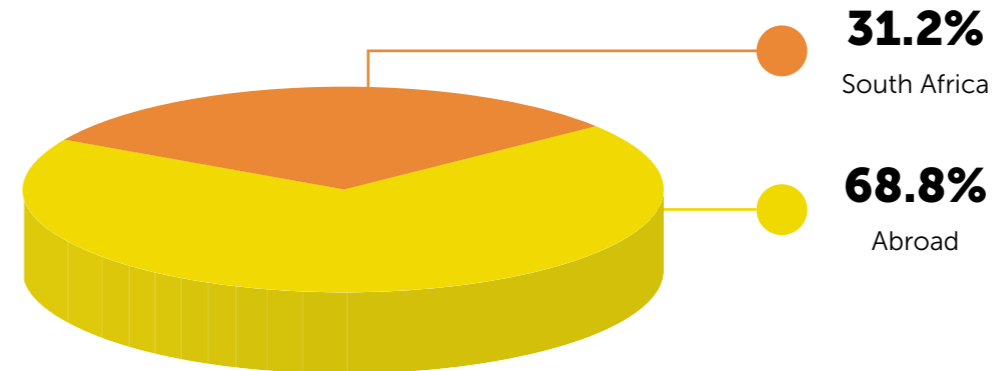


Prominent merchant groups were:

- Direct Marketing
- Taxicabs
- Security Brokers
- Airlines
- Hotels
- Clothing Stores

Credit

In **2018** **68.8%** of CNP credit card fraud occurred abroad.



Prominent merchant groups were:

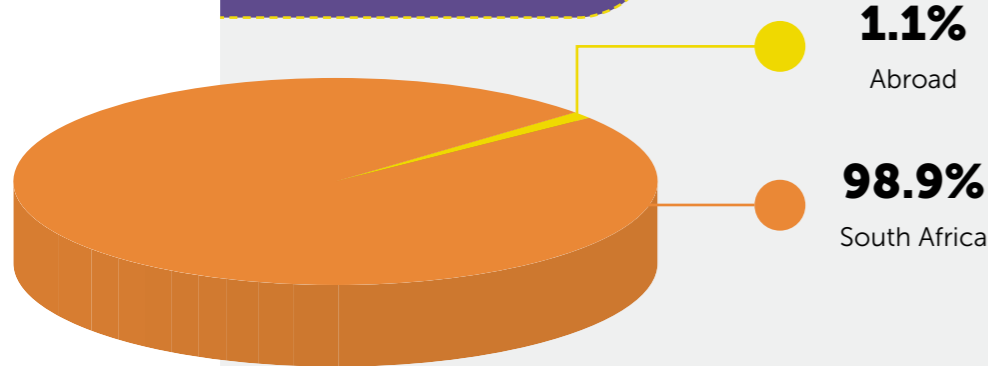
- Hotels
- Airlines
- Direct Marketing
- Travel Agencies
- Taxicabs
- Utilities (e.g. electricity)

Lost and/or Stolen

| PRODUCT | 2017 | 2018 | Inc/Dec | L&S as % of Gross Fraud |
|---------|--------------|--------------|-----------------|-------------------------|
| Debit | R178 428 112 | R165 895 846 | -7% decrease | 42.6% |
| Credit | R29 204 814 | R13 165 889 | -54.9% decrease | 2.7% |

Debit

In 2018 98.9% of Lost and/or Stolen debit card fraud occurred in South Africa.



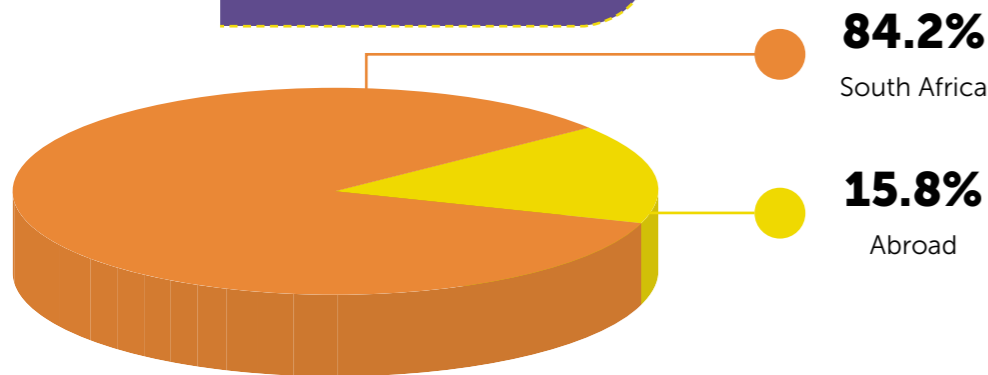
Prominent merchant groups were:

- ATMs
- Tollgates
- Liquor Stores
- Supermarkets
- Drinking Places
- Service Stations

70.5% of the gross fraud losses on Lost and/or Stolen debit cards were ATM withdrawals.

Credit

In 2018 84.2% of Lost and/or Stolen credit card fraud occurred in South Africa.



Prominent merchant groups were:

- Tollgates
- ATMs
- Liquor Stores
- Supermarkets
- Drinking Places
- Service Stations

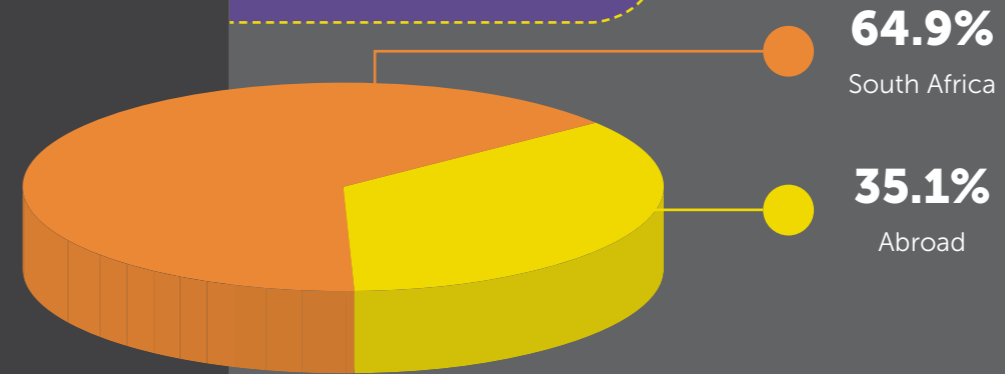
24.3% of the gross fraud losses on Lost and/or Stolen cards took place at a tollgate.

Counterfeit

| PRODUCT | 2017 | 2018 | Inc/Dec | Ctf as % of Gross Fraud |
|---------|-------------|-------------|-----------------|-------------------------|
| Debit | R62 230 192 | R76 440 677 | +22.8% increase | 19.6% |
| Credit | R69 225 166 | R66 990 516 | -3.2% decrease | 13.9% |

Debit

In 2018 64.9% of Counterfeit debit card fraud occurred in South Africa.



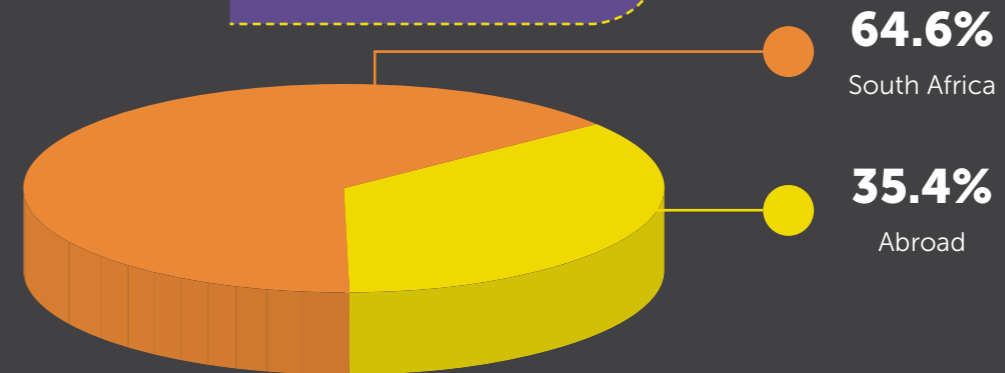
Prominent merchant groups were:

- ATMs
- Supermarkets
- Service Stations
- Automotive Parts
- Liquor Stores
- Restaurants

34.4% of the gross fraud losses on debit cards took place at an ATM.

Credit

In 2018 64.6% of Counterfeit credit card fraud occurred in South Africa.

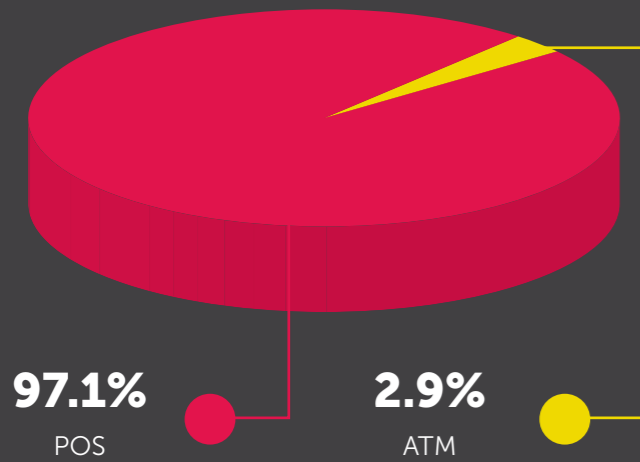


Prominent merchant groups were:

- Service Stations
- ATMs
- Supermarkets
- Automotive Parts
- Department Stores
- Restaurants

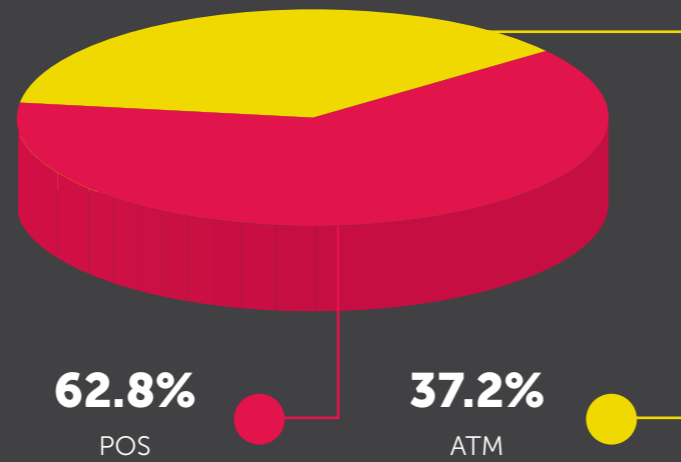
Card Fraud: ATM vs POS

Credit Card



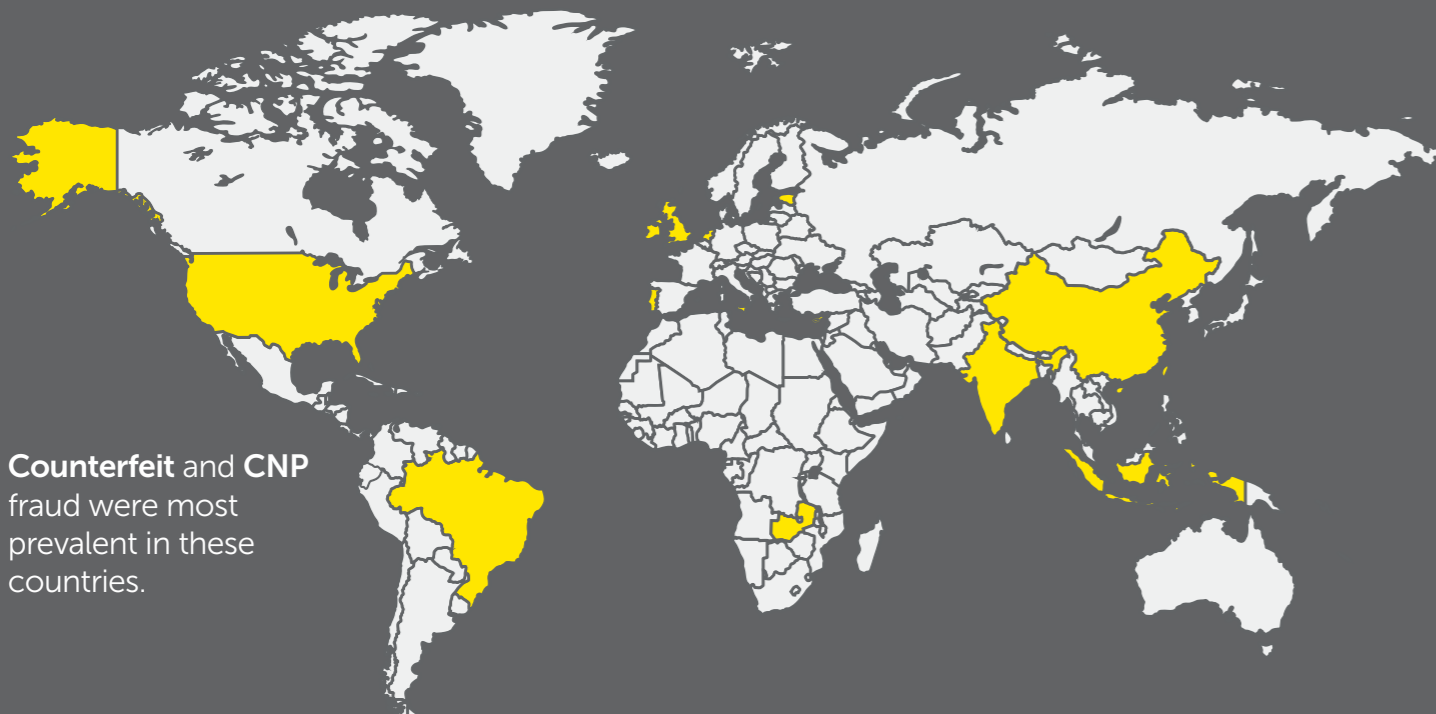
Transactions at Point of Sale (POS) devices amounted to **97.1%** of credit card fraud when compared to withdrawals at an ATM.

Debit Card



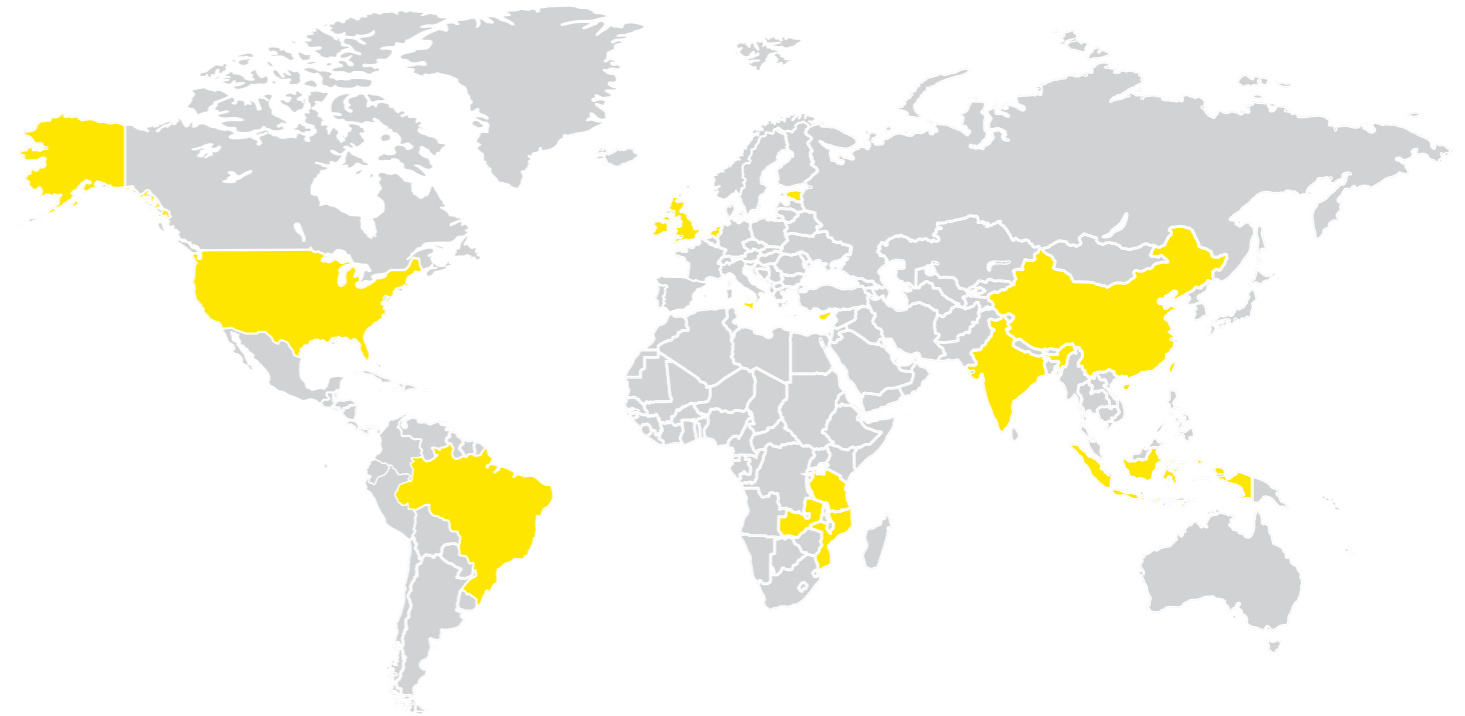
Debit card fraud at ATMs amounted to **37.2%** of gross fraud losses when compared to POS (**62.8%**) transactions.

International Perspective: SA Issued Credit Cards



- | COUNTERFEIT | | CNP | |
|------------------|--------------|------------------|---------------|
| ● UNITED STATES | ● IRELAND | ● UNITED KINGDOM | ● NETHERLANDS |
| ● INDONESIA | ● LUXEMBOURG | ● UNITED STATES | ● CYPRUS |
| ● UNITED KINGDOM | ● PORTUGAL | ● IRELAND | ● MALTA |
| ● INDIA | ● BRAZIL | ● LUXEMBOURG | ● CHINA |
| ● NETHERLANDS | ● ZAMBIA | ● ESTONIA | ● BRAZIL |

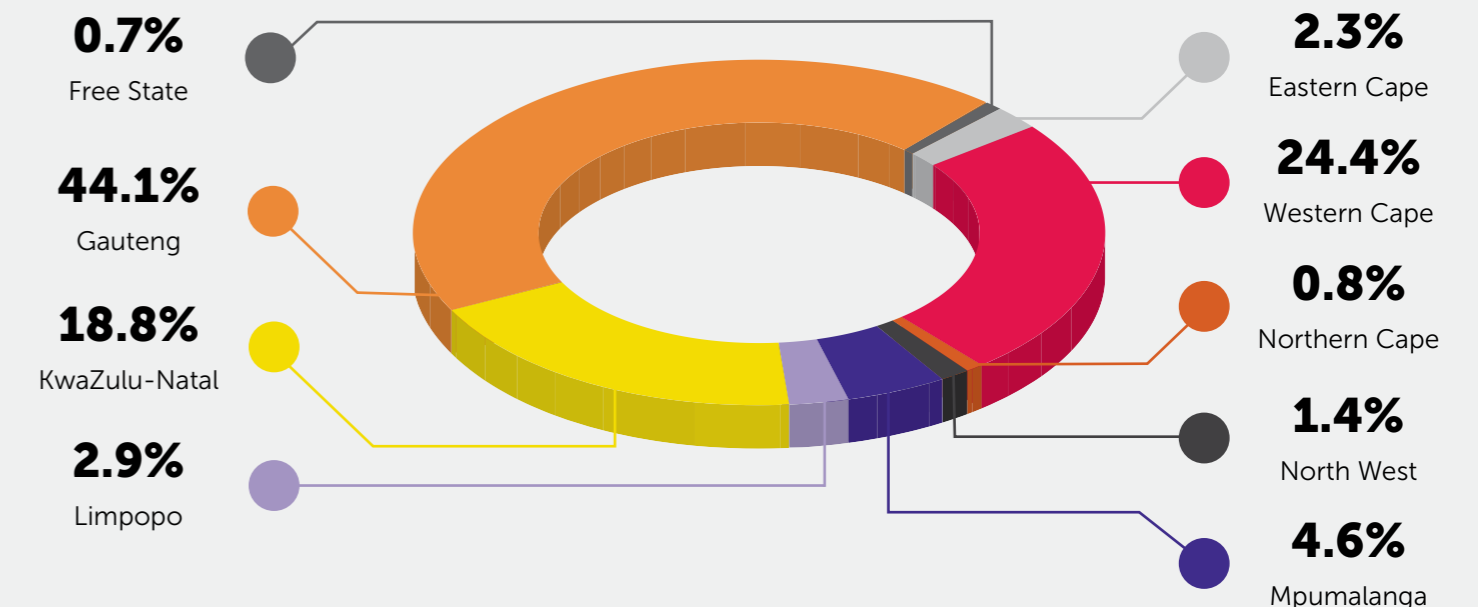
International Perspective: SA Issued Debit Cards



- | COUNTERFEIT | | CNP | |
|------------------|--------------|------------------|---------------|
| ● INDONESIA | ● MOZAMBIQUE | ● UNITED KINGDOM | ● NETHERLANDS |
| ● INDIA | ● ZAMBIA | ● UNITED STATES | ● ESTONIA |
| ● UNITED STATES | ● TANZANIA | ● IRELAND | ● BRAZIL |
| ● UNITED KINGDOM | ● BRAZIL | ● LUXEMBOURG | ● MALTA |
| ● CHINA | ● IRELAND | ● CYPRUS | ● CHINA |

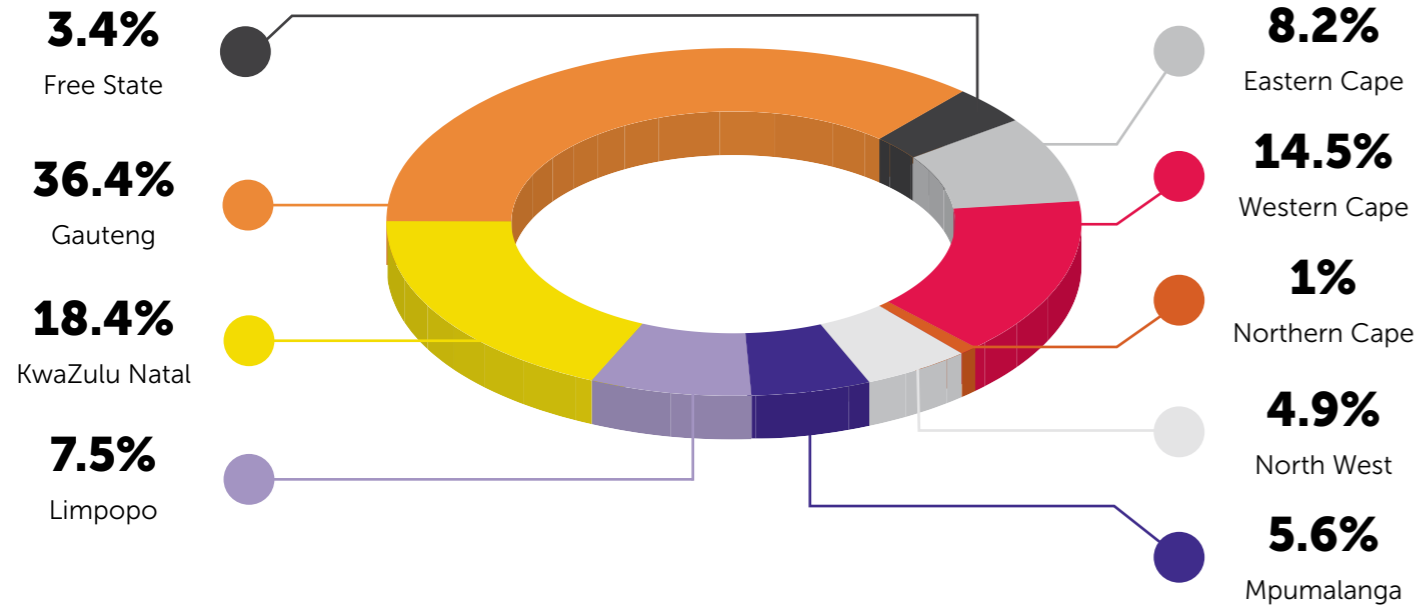
Provincial Overview

2018 saw Gauteng most affected by credit card fraud (**44.1%**), followed by the Western Cape (**24.4%**) and KwaZulu-Natal (**18.8%**).



The top three provinces affected by debit card fraud during 2018 were Gauteng (36.4%), KwaZulu-Natal (18.4%) and the Western Cape (14.5%).

Debit Card



84% of fraudulent transactions in South Africa took place with a Lost and/or Stolen debit card.

Find us Online



2018