ANNUAL CRIME STATISTICS 2024

SABRIC
South African Banking Risk Information Centre

CONTENTS

EXECUTIVE SUMMARY

The South African Banking Risk Information Centre (SABRIC) remains dedicated to its mission to support the banking and broader financial services industry in combating fraud and organised crime through effective information sharing, collaboration, and the strategic use of technology. As financial crime continues to evolve in complexity and sophistication, SABRIC's vision of enabling a safe and secure banking environment for all South Africans remains central to our mandate.

This report contains the SABRIC Annual Crime Statistics for 2024, providing a comprehensive analysis of financial crime trends and patterns, which is instrumental in informing targeted strategies and collaborative efforts to effectively mitigate crime and enhance security across South Africa's banking sector.

In 2024, financial crime continued to escalate, with significant increases in digital banking fraud, application fraud, and card-related crime. Emerging technologies, particularly generative artificial intelligence (AI), have been leveraged by criminals to craft more sophisticated fraud schemes, which has been evident in the unprecedented **86%** increase in digital banking fraud incidents and a **74%** rise in associated losses, totalling **R1.888 billion (bn)**. AI-driven scams, phishing campaigns, and deepfake-enabled impersonations emphasised the critical need for adaptive, intelligence-led security strategies.

Despite these challenges, the banking sector has made notable strides in mitigating contact crime. Associated robbery incidents declined by **35%**, with client losses reduced by **64%** compared to 2023. The successful collaboration between banks and the South African Police Service (SAPS), particularly through initiatives like the Associated Robbery Project, was instrumental in these achievements. Enhanced security protocols at branches and the proactive identification of suspects contributed significantly to this outcome. Additionally, the **18%** decrease in ATM attack explosive incidents can be attributed to the formation of a task team consisting of key stakeholders from various industries and law enforcement to combat these threats through data-driven intelligence and cross-sector collaboration.

Application fraud, however, saw a sharp rise, particularly within the Vehicle Asset Finance (VAF) stream, which recorded a **49.6%** increase in incidents and a **71.1%** increase in potential losses, totalling **R23 bn**. Modus operandi such as vehicle cloning and illegal changes of vehicle ownership continue to challenge stakeholders. The use of synthetic identities, AI-generated documents, and cross-border laundering further emphasises the growing sophistication of fraud rings. Unsecured credit fraud also surged, with a **57.6%** increase in reported cases and a corresponding **62.4%** increase in potential losses. While banks were able to prevent many of these applications, actual losses still more than doubled. Similarly, gross card fraud losses increased by **26.2%** year-on-year, reaching **R1.466 bn** in 2024, with "card-not-present" fraud remaining the dominant threat vector.

SABRIC acknowledges that these trends represent not only technological but also behavioural challenges, with social engineering attacks exploiting human error as a primary vulnerability. Multi-factor authentication, biometric verification, and increased public awareness remain key deterrents.

As we navigate an increasingly complex risk environment, SABRIC reaffirms its commitment to innovation, operational resilience, and industry collaboration. In 2024, the banking sector's unified efforts, alongside strategic partnerships with law enforcement, regulators, and private sector entities, enabled us to proactively detect, disrupt, and respond to criminal threats.

We commend the tireless efforts of our partners, members, and stakeholders. Through ongoing cooperation and the strategic embrace of technology, we will continue to evolve in our efforts to safeguard South Africa's banking infrastructure and the customers it serves.

MEMBERS

absa

NEDBANK

alBaraka

FNB

TymeBank

Standard Bank

Postbank
A member of the Post Office group

access

Investec

ria Money Transfer

African Bank

Discovery Bank

CAPITEC BANK

Bidvest Bank

Lesaka

PARTNERS

Public Sector

- HAWKS DIRECTORATE FOR PRIORITY CRIME INVESTIGATION
- National Prosecuting Authority of South Africa
- state security State Security Agency REPUBLIC OF SOUTH AFRICA
- Eskom
- CSIR Touching lives through innovation
- communications & digital technologies Department: Communications and Digital Technologies REPUBLIC OF SOUTH AFRICA
- home affairs Department: Home Affairs REPUBLIC OF SOUTH AFRICA
- the doj & cd Department: Justice and Constitutional Development REPUBLIC OF SOUTH AFRICA
- FIC Financial Intelligence Centre

Private Sector

- Provenance
- LUNO
- iiDENTIFii
- kaspersky
- BANKSERVAFRICA

Universities

- UNIVERSITEIT VAN PRETORIA UNIVERSITY OF PRETORIA YUNIBESITHI YA PRETORIA
- MANDELA INSTITUTE

Industry Bodies/ Associations

- SADC BANKING ASSOCIATION
- THE BANKING ASSOCIATION SOUTH AFRICA
- consumer goods council of south africa Helping members trade better.
- COMRiC
- CITASA
- ISPA INTERNET SERVICE PROVIDERS' ASSOCIATION
- ASISA
- INSURANCE CRIME BUREAU INTELLIGENCE THAT WORKS

QUALIFICATION OF INFORMATION

The information utilised in this publication was provided by SABRIC members. The statistics used in the report cover the period, 1 January to 31 December 2023 and 2024. The statistics contained in this publication may differ slightly from previous publications due to the continuous reporting of information post-publication, regular data verification processes followed by SABRIC, as well as ongoing investigations.

The information used was as follows:

- For the comparative analysis, 2023 was compared to 2024.
- All calculations are based on the date that the incident or fraudulent transaction occurred.
- All contact crime losses mentioned in this publication refer to cash that was robbed or stolen and excludes cash that was recovered or other damages that were incurred.
- All fraud losses mentioned in this publication refer to gross fraud losses.
- Loss figures are rounded to the nearest **R1 million (m)**, unless otherwise stated and therefore the sum of the separate losses (for example per loss category/fraud type) may differ from the rounded loss reflected.

TOTAL FINANCIAL CRIME 2024 AT A GLANCE

Year	Total (Potential) Losses Reported to SABRIC*	Actual Losses*	Reported Cases/Incidents/Transactions*
2024	R30 739 895 830	R 2 721 652 072	2 074 059

Table 1: Total Financial crime 2024

**The categorisation is based on inputs as per reporting bank protocols and definitions are not necessarily comparable between crime types.*

TOTAL/POTENTIAL LOSSES:

Refer to the estimated financal impact that occurred due to fraud and represents what crimminals attempted to steal, but may have been unsuccessful in doing so.

ACTUAL LOSSES:

Are the real, confirmed financial damage incurred as a result of fraudulent criminal activities.
They include the immediate monetary amount that was stolen, or the value of transactions that were executed fraudulently, including unauthorised transfers.

BREAKDOWN OF FINANCIAL CRIME PER CRIME TYPE

APPLICATION FRAUD

2024	Potential Loss	Actual Loss	Incident Count
Jan	R 2,132,903,924.47	R 36,409,311.02	10063
Feb	R 2,427,575,817.95	R 84,743,501.33	10186
Mar	R 2,124,032,415.15	R 66,058,438.00	10419
Apr	R 2,623,213,935.24	R 47,126,535.73	11197
May	R 2,252,833,792.19	R 46,953,916.40	9853
Jun	R 2,303,622,662.28	R 35,046,745.70	8866
Jul	R 3,262,580,089.00	R 32,105,557.72	10086
Aug	R 2,924,050,502.91	R 95,862,872.50	9727
Sep	R 1,977,465,363.03	R 74,505,801.00	8361
Oct	R 2,960,244,912.09	R 125,132,091.00	10114
Nov	R 3,033,720,211.57	R 106,919,995.67	10224
Dec	R 2,717,652,205.03	R 46,630,566.67	8754
Total	**R 30,739,895,830.91**	**R 797,495,332.74**	**117850**

CONTACT CRIME

2024	Potential Loss	Actual Loss	Incident Count
Jan		R3,021,006	55
Feb		R3,620,165	54
Mar		R2,866,420	42
Apr		R2,376,310	41
May		R4,353,279	62
Jun		R3,500,890	62
Jul		R2,950,326	83
Aug		R2,096,713	75
Sep		R2,350,140	79
Oct		R4,457,880	86
Nov		R7,158,687	85
Dec		R1,604,440	26
Total	**N/A**	**R40,356,256**	**750**

DIGITAL BANKING CRIME

2024	Potential Loss	Actual Loss	Incident Count
Jan		R 102 391 073.00	5593
Feb		R 129 747 274.00	5694
Mar		R 101 896 578.00	6253
Apr		R 111 959 488.00	7051
May		R 166 691 456.00	9756
Jun		R 192 087 478.00	8903
Jul		R 197 240 453.00	8791
Aug		R 176 913 263.00	9583
Sep		R 177 844 675.00	8912
Oct		R 194 296 748.00	10778
Nov		R 176 160 316.00	8586
Dec		R 156 571 682.00	8059
Total	**N/A**	**R 1 883 800 484.00**	**97959**

CARD FRAUD

2024	Gross Fraud Losses (Debit & Credit): Potential	Actual Loss	Transactions
Jan	R120,898,408		157,502
Feb	R105,232,119		127,326
Mar	R123,689,839		156,083
Apr	R134,128,509		169,561
May	R123,029,874		172,571
Jun	R112,428,304		157,813
Jul	R120,363,387		163,377
Aug	R96,872,208		139,156
Sep	R113,267,643		138,708
Oct	R140,297,329		145,664
Nov	R135,190,909		161,132
Dec	R140,900,244		168,607
Total	**R1,466,298,773**	**N/A**	**1,857,500**

CONTACT CRIME

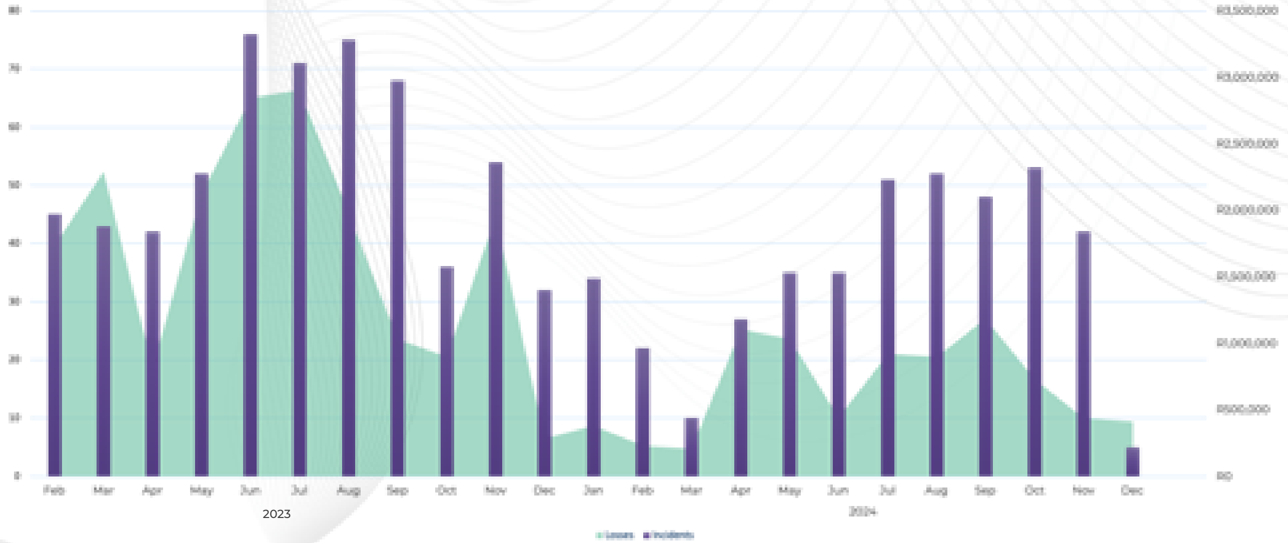
ASSOCIATED ROBBERY

The industry recorded a **35%** decrease in associated robbery incidents during 2024, and a subsequent **64%** decrease in accompanying losses to clients compared to 2023. The notable decline in related robbery incidents is largely due to a collaborative project between the banking industry and the South African Police Service (SAPS), aimed at sharing information on identified suspects and alerting authorities when these individuals entered bank branches, enabling the identification of potential cash-withdrawal victims.. Associated Robbery inside a branch decreased by **96%** resulting in only one reported incident during 2024. The decrease can directly be attributed to the Associated Robbery project that led to the arrest of several suspects linked to inside branch robberies.

Associated robberies pose a significant reputational risk to businesses, as clients who experience losses may lose trust in the company's ability to protect their interests. When clients suffer financial or material losses due to such incidents, it can lead to negative publicity and diminished customer confidence.

Clients making cash deposits at ATM machines are perceived as easy targets for criminals, especially during the first six days of the month in which grant payments are paid out. This serves as a driving factor for the **66%** increase in associated robbery incidents for the reporting time period.

Criminals take advantage of the clients' ignorance and superstitions by using tactics such as smearing muti on them to extort money, or employing a "money bomb" scam where cash is dropped on the ground to trick victims into handing over more money. Associated robbery incidents are often categorised as common robbery and aggravated robbery by the SAPS, making it difficult to distinguish them from associated robberies. Furthermore, some victims report incidents to a bank branch instead of the SAPS.



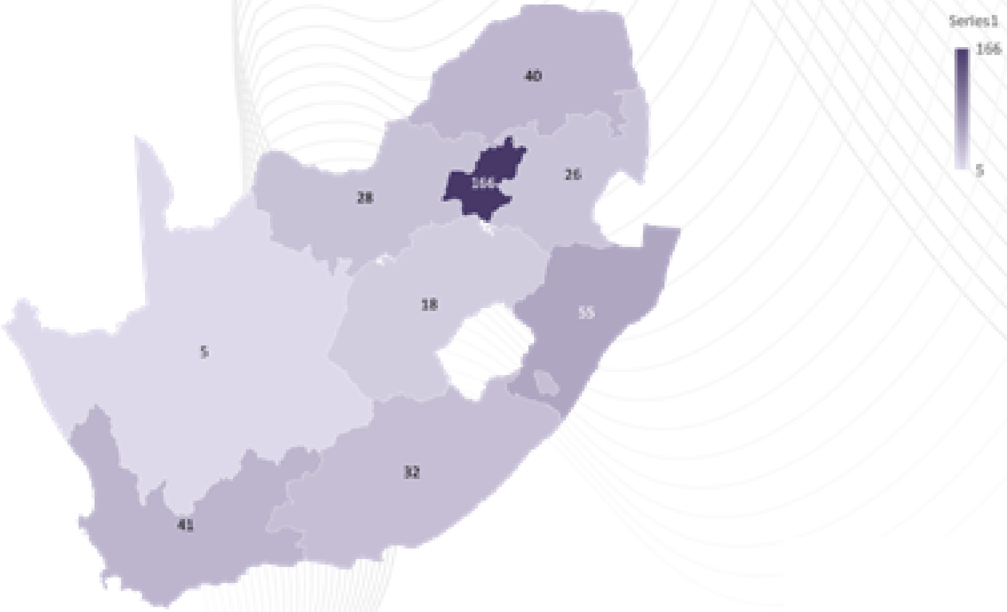
Graph 1: Associated Robery incidents and loss for reporting period 2023 and 2024

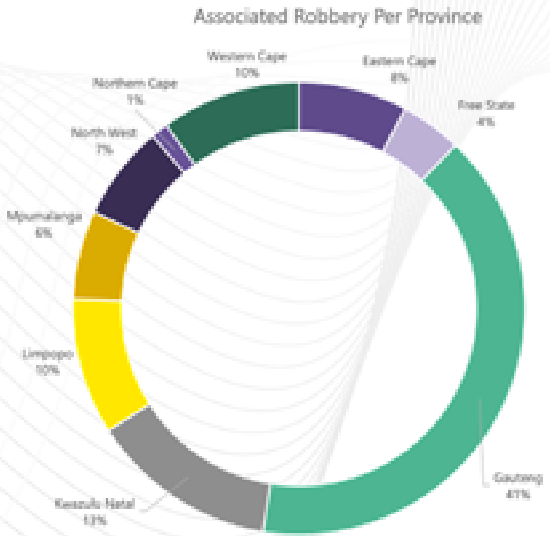
Incident Sub-Type	Incidents			Cash Loss		
	2023	2024	% Diff	2023	2024	% Diff
Associated Robbery - Branch Before Deposit	116	26	-78%	R8,078,411	R1,956,916	-76%
Associated Robbery - ATM After Withdrawal	256	154	-40%	R1,736,937	R537,405	-69%
Associated Robbery - ATM before Deposit	47	78	66%	R494,000	R1,339,895	171%
Associated Robbery - Branch After Withdrawal	120	55	-54%	R6,346,453	R2,941,595	-54%
Associated Robbery - Cash Centre After Withdrawal	1	0	-100%	R126,300	R0	-100%
Associated Robbery - Inside Branch	25	1	-96%	R2,919,142	R100,000	-97%
Associated Robbery - Other - Money bomb	30	64	113%	R155,516	R358,657	131%
Associated Robbery - Other - Muti	18	22	22%	R608,077	R591,471	-3%
Associated Robbery - Other - Theft out of vehicle	1	0	-100%	R1,600,000	R0	-100%
Associated Robbery Other (Determined by MO)	20	14	-30%	R297,260	R150,500	-49%
Total	**634**	**414**	**-35%**	**R22,362,096**	**R7,976,439**	**-64%**

Table 2: Associated Robery incidents and cash loss 2023-2024

Enhanced security measures implemented at branches serve as a driver for the **78%** decrease in the sub-type of branch before deposit incidents in 2024, financial losses in the same category decreased by **76%** when compared to 2023. These security measures led to less loitering, in turn keeping clients safe from criminals attempting to monitor those depositing large amounts of cash.

The arrest of the main suspects as well as the sharing of information to branches also contributed to a decrease in reported incidents.





Gauteng was the province with the highest number of reported Associated Robbery incidents ***(41%)*** *followed by KwaZulu Natal* ***(13%).***

Figure 1: Associated Robery incidents and loss for reporting period 2023 and 2024 on map provincial layout

Province	Incidents			Cash Loss		
	2023	2024	2024	2023	2024	2024
Eastern Cape	72	32	-56%	R2,038,030	R520,720	-74%
Free State	35	18	-49%	R422,987	R70,700	-83%
Gauteng	251	166	-34%	R11,621,031	R4,619,199	-60%
Kwazulu Natal	72	55	-24%	R1,308,090	R814,739	-38%
Limpopo	53	40	-25%	R1,876,932	R387,737	-79%
Mpumalanga	43	26	-40%	R2,118,091	R361,730	-83%
North West	49	28	-43%	R1,695,948	R144,314	-91%
Northern Cape	5	5	0%	R43,324	R22,400	-48%
Western Cape	54	41	-24%	R1,237,663	R774,900	-37%
Total	**634**	**414**	**-35%**	**R22,362,096**	**R7,976,439**	**-64%**

Table 4: Associated Robery incidents and loss provincial

International Perspective Associated Robbery

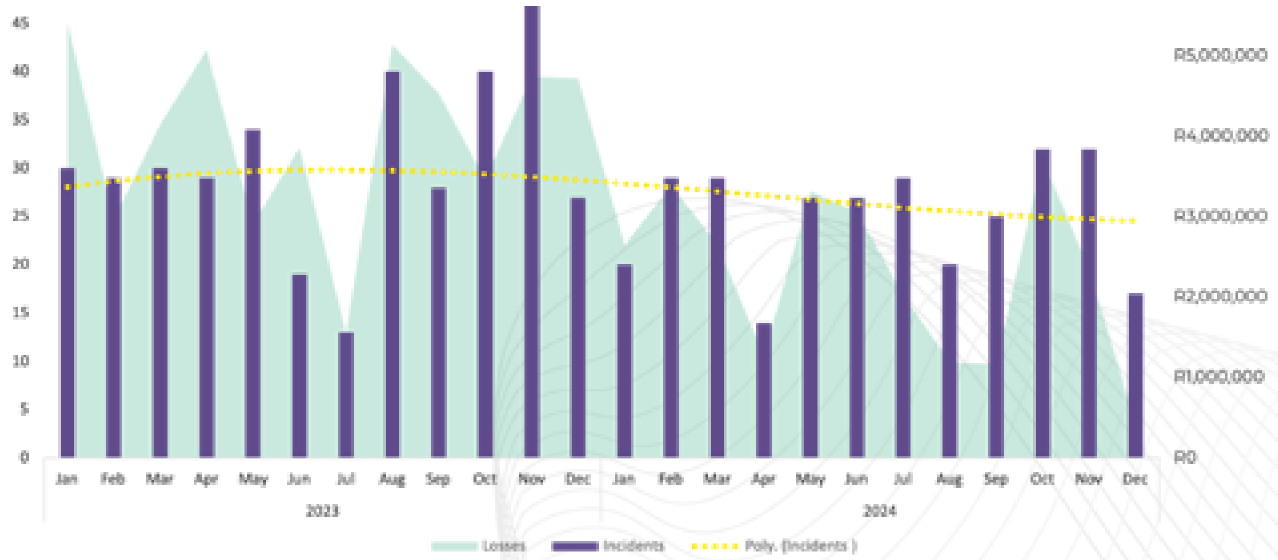
The term **"associated robbery"** are commonly used in South Africa although the crime type features globally under different terminology. Globally, the same phenomenon is known under different names; In the United States, they are called **"Follow-home robberies"** or **"bank jugging",** while in the United Kingdom it is known as **"Distraction thefts"**. In the Latin American region, a translation of **"bank marking"** called **"Marcaje bancario"** is used to describe this type of crime.

These incidents follow a similar pattern in its execution, where criminals surveil and observe bank customers to identify potential targets. These attacks also occur shortly after a withdrawal or before a deposit, and victims are targeted in a variety of areas including parking lots, at home, or en route. A certain level of violence is accompanied with these incidents, especially if the victim resists.

To reduce the risk of becoming a victim of associated robberies, consider following these prevention measures;

- Avoid routine banking patterns.
- Use electronic transfers and digital payment methods instead of carrying cash.
- Be aware of the surroundings when leaving a bank or ATM.
- Use secure cash-in-transit services for businesses.

ATM Attack



Graph 2: ATM attacks 2023 & 2024

An **18%** decrease in ATM attacks during 2024 was reported by the industry, resulting in a **44%** decrease in cash losses. **74%** of the reported incidents can be attributed to SABRIC member banks, while the remaining **26%** were reported by non-SABRIC member institutions.

Incident Sub-Type	Incidents			Cash Loss		
	2023	2024	% Diff	2023	2024	% Diff
ATM Attack - Burglary	11	21	91%	R0	R0	0%
ATM Attack - Cutting Torch	5	1	-80%	R498,430	R0	-100%
ATM Attack - Explosives	308	254	-18%	R41,582,088	R24,901,010	-40%
ATM Attack - Grinder	26	16	-38%	R5,376,510	R2,092,150	-61%
ATM Attack - Theft	1	3	200%	R0	R0	0%
ATM Attack - Tools	15	6	-60%	R1,056,230	R246,680	-77%
Total	**366**	**301**	**-18%**	**R48,513,258**	**R27,239,840**	**-44%**

Table 5: ATM attacks 2023 & 2024

Incidents of ATM attacks committed through explosives decreased by **18%** during 2024 when compared to 2023. Of the reported incidents, SABRIC member banks accounted for **74%** of occurrences, while non-SABRIC institutions reported the remaining **26%**. In **85%** of the ATM attack-explosives incidents, the perpetrators were successful in accessing the cash, despite the activation of dye-stain technology. Gauteng Province reported the most ATM attack-explosives incidents at a rate of **67%**, followed by Limpopo Province at a rate of **9%**. The Southern parts of Gauteng were most affected by ATM attack-explosives incidents with Johannesburg District at a rate of **45%** and Ekurhuleni at a rate of **38%**. The use of explosives to attack an ATM makes it possible for the perpetrators to execute the operation quickly, especially when targeting service stations where there are two or more ATM machines. The perpetrators have, in some instances, also robbed the service station shop and also attacked the drop safes at the service station.

Incidents of ATM attacks commited through an Angle Grinder decreased by **38%** from 26 during 2023 to 16 incidents in2024. In **82%** of the ATM attack grinder incidents, the perpetrators were successful in accessing the cash in the ATM whether it was dye stained or not. Usually, the perpetrators will target a shopping center to hold security guards hostage and the perpetrators, dressed in guard uniform, will keep a lookout on the outside while the rest of the perpetrators will use grinders to access the ATM cash. The grinding of an ATM attack indicates a coordinated approach as a large group of perpetrators, time, and planning is required . The risk to perpetrators is high due to prompt responses from reaction teams that respond after alarm signal loss. It seems that during load shedding the perpetrators could limit the impact due to signal loss and perpetrators dressed as guards indicating to reaction teams that all was in order.

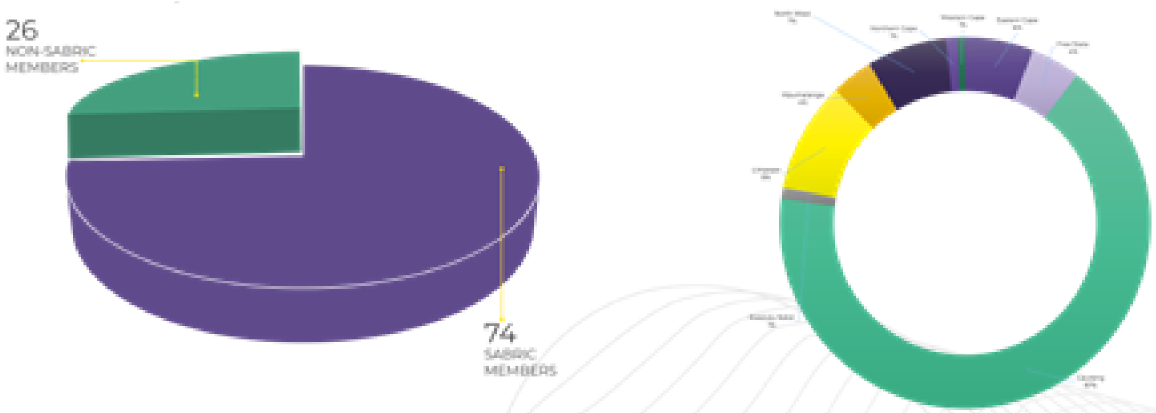


Figure 2 : ATM attacks: Explosive-SABRIC members vs Non SABRIC members

Province	Incidents			Cash Loss		
	2023	2024	% Diff	2023	2024	% Diff
Eastern Cape	14	18	29%	R613,960	R816,370	-33%
Free State	32	13	-59%	R824,420	R1,179,890	-43%
Gauteng	224	201	-10%	R34,540,009	R20,257,880	-41%
Kwazulu Natal	5	3	-40%	R392,960	R0	-100%
Limpopo	32	29	-9%	R3,498,220	R2,454,940	-30%
Mpumalanga	29	11	-62%	R4,952,429	R1,134,260	-77%
North West	23	21	-9%	R3,658,790	R1,396,500	-62%
Northern Cape	1	3	200%	R32,470	R0	-100%
Western Cape	6	2	-67%	R0	R0	0%
Grand Total	**366**	**301**	**-18%**	**R48,513,258**	**R27,239,840**	**-44%**

Table 6: ATM attacks incidents and loss 2023 & 2024

The **18%** decrease in ATM Attack explosive incidents can be attributed to the formation of a task team consisting of key stakeholders from various industries and law enforcement to combat these threats through data-driven intelligence and cross-sector collaboration.

The majority of ATM attacks occurred in Gauteng at a rate of **67%**, followed by Limpopo province at **9%** and the North West province at **7%**. ATM Attack incidents in the Eastern Cape province increased by **29%** during 2024 compared to 2023.

International Perspective on ATM Attacks

ATM Attacks are a global phenomenon and based on recent reports, it was stated that there is a continued global threat from both physical and fraud-based ATM attacks (ATMIA, 2024).

Additionally, physical attacks (including ram raids and explosive attacks) remain a major concern.

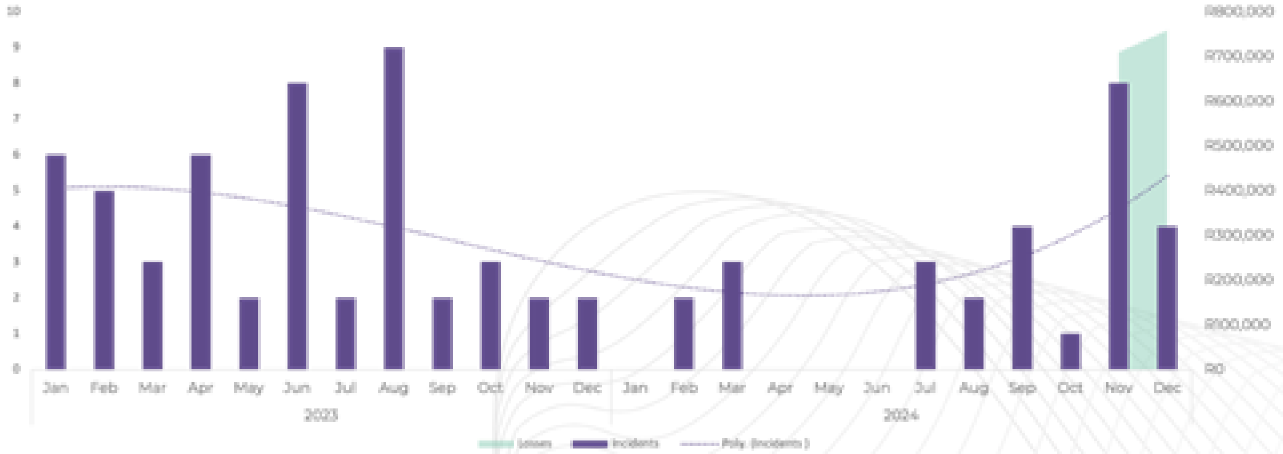
Emerging threats include hybrid attacks combining physical and digital methods.

The European Association for Secure

Transactions (EAST), in their 2023/2024 report reported that ATM physical attacks rose by **24%**, indicating an increase from **3,728** to **4,637** incidents for the same time period, while explosive attacks slightly decreased by **2% (714 incidents)** but still caused **€5.36 m** in losses.

While 2024-specific statistics are limited, trends from 2019–2022 highlighted a **600%** increase in ATM attacks from 2019 to 2022 across the United States, where an average of **$27,000** stolen per attack, with **$50,000+** reported in replacement costs 3. Attacks often involved vehicle-assisted thefts and black box attacks (malware-based cash-outs).

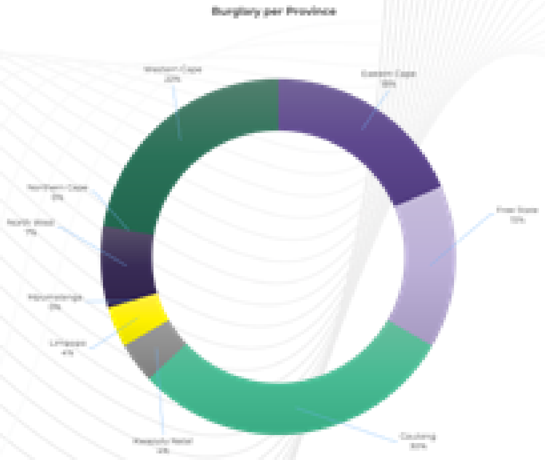
Burglary – Commercial Retail Banking Industry



Graph 3: Burglary – commercial retail banking industry 2023-2024

A well-known modus operandi of criminals accessing the back of the bank branch and climbing onto the roof to cut through the corrugated iron to access the branch became prominent again during 2024. Jackhammers and grinders would then be used to breach the safe.

Gauteng (8 incidents), Western Cape (6 Incidents) and Eastern Cape (5 incidents) were the provinces with the highest number of reported branch burglary incidents.



Despite a significant **46%** decrease in bank branch burglary incidents in 2024, the related cash losses increased by **226%** during 2024. Three incidents where cash was targeted during a burglary were reported in 2024. Perpetrators also targeted assets such as laptops and computers. In **56%** of the burglary incidents nothing was stolen.

Incident Sub-Type	Incidents			Cash Loss		
	2023	2024	% Diff	2023	2024	% Diff
Burglary - Asset	18	3	-83%	R0	R0	0%
Burglary - Cash	9	3	-67%	R449,950	R1,467,620	226%
Burglary - Computer	2	6	200%	R0	R0	0%
Burglary - Nothing Stolen	21	15	-29%	R0	R0	0%
Burglary Total	**50**	**27**	**-46%**	**R449,950**	**R1,467,620**	**226%**

Table 7: Burglary – commercial retail banking industry 2023-2024

Province	Incidents			Cash Loss		
	2023	2024	% Diff	2023	2024	% Diff
Eastern Cape	10	5	-50%	R0	R1,467,620	100%
Free State	6	4	-33%	R0	R0	0%
Gauteng	10	8	-20%	R449,950	R0	-100%
Kwazulu Natal	5	1	-80%	R0	R0	0%
Limpopo	1	1	0%	R0	R0	0%
Mpumalanga	5	0	-100%	R0	R0	0%
North West	7	2	-71%	R0	R0	0%
Northern Cape	0	0	0%	R0	R0	0%
Western Cape	6	6	0%	R0	R0	0%
Burglary Total	**50**	**27**	**-46%**	**R449,950**	**R1,467,620**	**226%**

Table 8: Burglary – commercial retail banking industry provincial

International Perspective on Bank Branch Burglaries

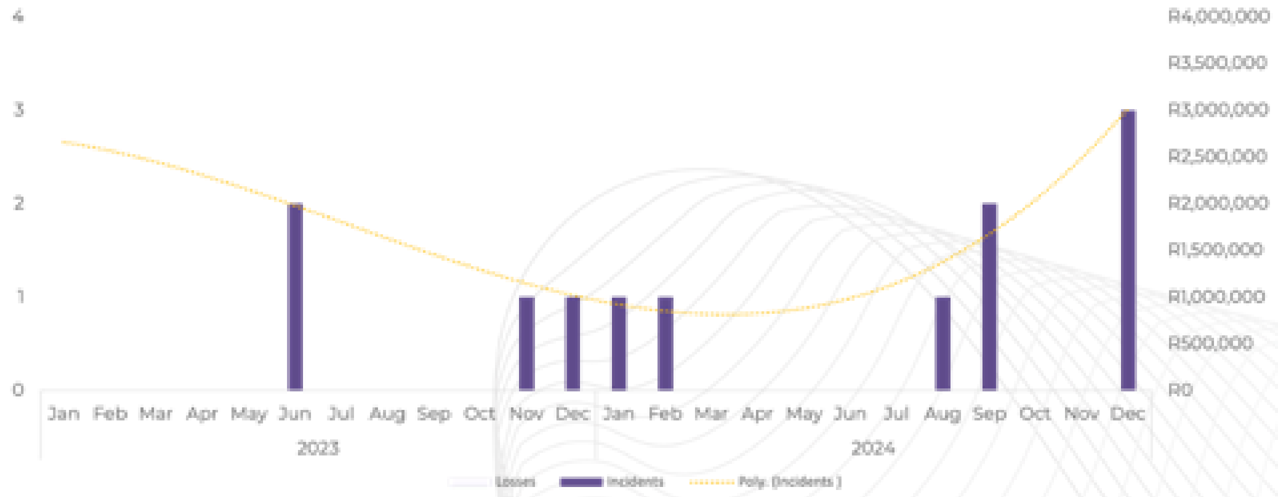
Many countries have reported a steady decline in physical bank branch burglaries over the past decade. This is largely due to several factors, including but not limited to:

- Increased use of digital banking.
- Enhanced security systems (e.g., CCTV, alarms, time-locked safes).
- Reduced cash holdings at branches.
- Shifts Toward Cybercrime.
- Criminals are increasingly targeting digital infrastructure rather than physical branches.
- Cyberattacks and fraud now account for a larger share of financial crime losses globally.

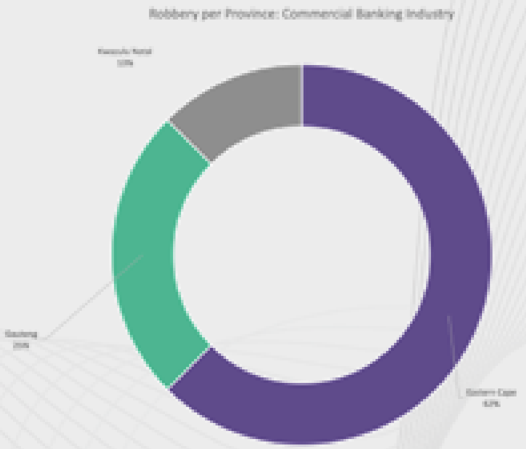
Globally, different trends has been noted regarding the occurrence of bank branch burglaries In Europe, countries such as Italy and the United Kingdom have seen significant decreases in bank burglaries, while in Latin America, some countries still report higher rates of physical attacks due to cash-heavy economies.

Across Africa and Asia, mixed trends were observed, with some areas experiencing increased attacks on rural or under-secured branches.

Robbery – Commercial Private Banking Industry



Graph 4: Robbery – Commercial Private Banking Industry



Incident Sub-Type	Incidents			Cash Loss		
	2023	2024	% Diff	2023	2024	% Diff
Robbery	4	8	100%	R834 084	R3 672 357	340%
	4	**8**	**100%**	**R834 084**	**R3 672 357**	**340%**

Table 9: Robbery – Assets incidents and loss

Eight bank robbery incidents were reported during 2024 compared to four incidents during 2023, indicating a **100%** increase. Opportunistic perpetrators targeted single tellers at bank branches located across the Eastern Cape (five incidents), Gauteng (two incidents) and KwaZulu-Natal (one incident) to obtain relatively low cash amounts kept in the teller drawers. . The traditional bank robbery incidents where a group of suspects would hold up staff and clients at gunpoint were unseen during 2023 and 2024 due to safety mitigation strategies implemented by the banks.

The Easten Cape **(62%)** and Gauteng Province **(25%)** were the provinces with the highest number of reported bank robbery incidents.

Province	Incidents			Cash Loss		
	2023	2024	% Diff	2023	2024	% Diff
Eastern Cape	1	5	400%	R803,044	R19,000	-98%
Free State	0	0	0%	R0	R0	0%
Gauteng	2	2	0%	R31,040	R3,653,357	11670%
Kwazulu Natal	0	1	100%	R0	R0	0%
Limpopo	0	0	0%	R0	R0	0%
Mpumalanga	0	0	0%	R0	R0	0%
North West	1	0	-100%	R0	R0	0%
Northern Cape	0	0	0%	R0	R0	0%
Western Cape	0	0	0%	R0	R0	0%
Grand Total	**4**	**8**	**100%**	**R834,084**	**R3,672,357**	**340%**

Table 10: Robbery– Assets incidents and loss provincial

International Perspective Bank Branch Robberies

According to the 2024 Global Financial Crime Report, physical bank robberies are declining globally, while cybercrime and fraud are on the rise.

Many countries report fewer in-person robberies due to several factors, including:

- Increased digital banking
- Enhanced security systems
- Reduced cash holdings at branches

The Federal Bureau of Investigation (FBI) Bank Crime Statistics for 2023 reported that more than **1500** bank robberies occurred involving note passing or threats of violence. Many of the incidents occurred in urban areas.

In Italy, the Italian Banking Association (ABI) reported a **36.3%** drop in bank robberies in 2024, indicating **80** incidents in 2023 to **51** in 2024, representative of the **93.6%** decrease in robberies over the past decade.

DIGITAL CRIME

In 2024, Digital banking crime continued to surge, following the sharp upward trend from 2023. Digital banking fraud incidents escalated in 2024 when compared to figures from the previous year, depicting an **86%** increase in reported incidents from the banking industry and **74%** increase in associated losses. This significant increase highlights the need for robust countermeasures.

Table 1 provides an overview of reported incidents and gross losses:

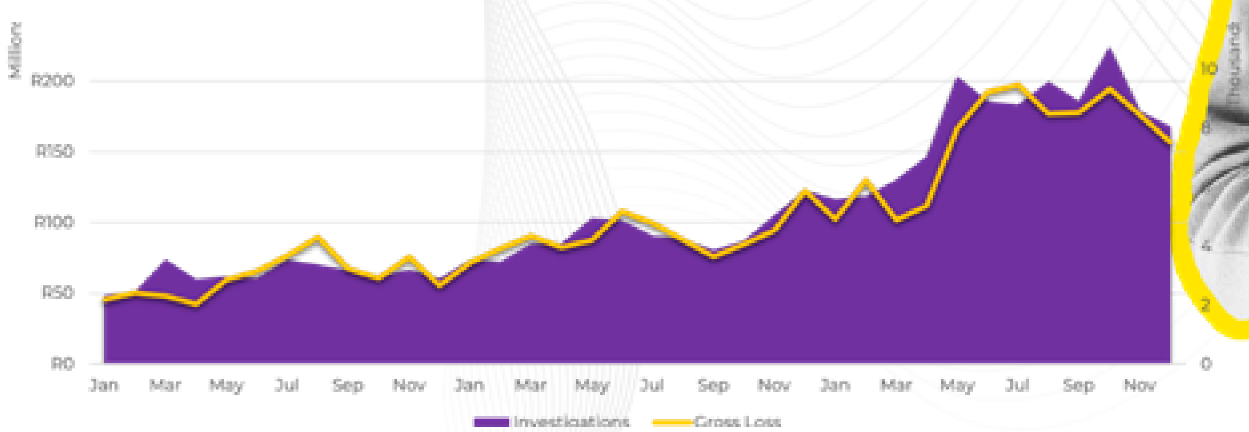
Year	Reported Incidents	YoY Change	Gross Fraud Losses	YoY Change
2022	36,178	–	R734.7 m	–
2023	52,584	+45%	R1.082 bn	+47%
2024	97,975	+86%	R1.888 bn	+74%

Table 11: Digital Banking Fraud in South Africa 2022–2024

Note: "YoY" = Year-over-Year change. 2022-2024 figures are verified totals reported by banks.

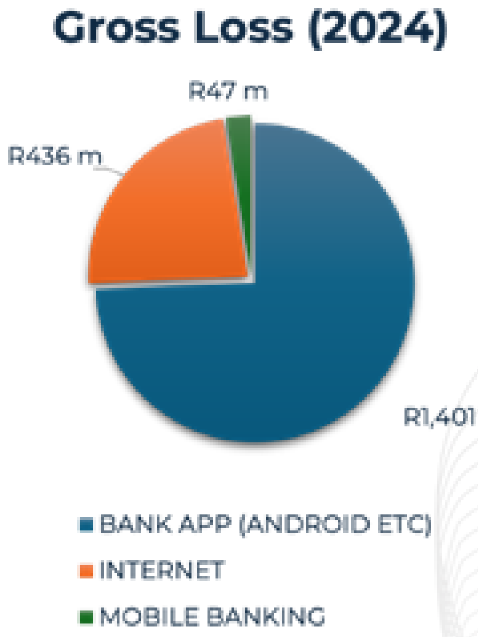
KEY TRENDS & STATISTICS (2022–2024)

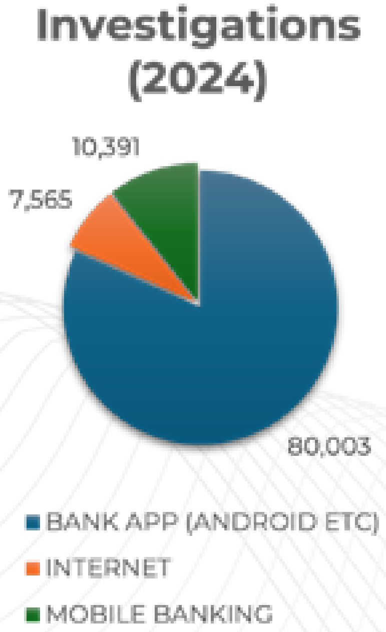
Digital banking fraud has spiked over the past three years, with 2024 seeing the highest volumes and losses on record thus far.



Graph 5: Digital Banking fraud reports investigations and losses in South Africa per month 2022–2024

Reported fraud Incidents nearly doubled in 2024, marked by a **86%** increase from 2023, reaching **97 975** reported cases. Gross losses spiked to approximately **R1.888 bn**, indicating a **74%** increase from 2023. This illustrates that more than half of the total digital banking fraud losses in the last three years occurred in 2024 alone.





Note: "Gross Loss" = displayed in millions

Banking apps as prime targets: Banking application (Android, etc) is the dominant channel utilised for fraud, accounting for **65.3%** of reported incidents in 2024. In 2023, banking app fraud made up **60%** of reported cases **(31 612** incidents**)**, nearly doubling to **~64,000** incidents in 2024. Losses from app fraud exceeded **R1.2 bn** in 2024, as compared to losses in 2023.

All reported incidents involved criminals exploiting human error through social engineering techniques to compromise accounts, as opposed to technical breaches of banking app platforms' security.

Other channels (online/USSD banking): Traditional internet banking and USSD-based mobile banking now form a smaller share of all reported incidents. Approximately **10%** of cases reported in 2024 involved internet web banking fraud **~8%** and **~9%** were USSD/older mobile banking fraud. While banking apps remain a prominent attack vector in 2024, fraud on all digital channels remains a concern.

Social engineering drives fraud: Human fallibility is a primary attack vector which is exploited to deploy social engineering attacks. The surge in fraud during 2024 was largely due to phishing, vishing, and other social engineering tactics. Criminals obtained passwords, PINs, or approvals by tricking victims through sophisticated fraud schemes, and in some cases, scams driven by Artificial Intelligence (AI).

2024 represented a year of exceptional growth in digital banking crime, with banking apps aggressively targeted. The convergence of several factors, including smartphone penetration, internet access and customer demand leading to increased digital banking coupled with easily accessible fraud kits to deploy sophisticated social engineering attacks resulted in the unprecedented increase in digital banking fraud.

Common Fraud Schemes and Modus Operandi during 2024

Criminals in 2024 continued to use a range of fraud modus operandi (MOs),– often combining multiple methods in one attack to ensure maximum effect. Below are the most prevalent scams and schemes containing an assessment of its typical features and any notable evolutions from 2023:

Social Engineering (Phishing/Vishing/ Smishing)

Exploiting trust and fear to obtain confidential information, criminals send emails, make calls or SMSs to steal credentials or deceive them into approving transactions or divulging their sensitive information, such as login information. These emails, calls or SMSs often resemble legitimate entities, with criminals using spoofed email addresses or names, increasing the likelihood that victims will hand over sensitive information. In other instances, criminals will send multiple emails, SMSs or calls at the same time to overwhelm the victim, tricking them into responding or confirming sensitive information in a tactic also known as spearphishing. In many reported cases, victims receive a fake email from seemingly their bank urging the victim to log in via a provided link, leading to a spoofed website that steals their username and password. Immediately after, a vishing call from a fake fraud department might trick the victim into divulging a one-time pin, which will be used to log in to the legitimate banking site and gain access to the victim's account. Vishing callers have become more sophisticated, sometimes knowing personal details due to data leaks or previous scams to obtain the details.

QR Code Phishing, more commonly known as Quishing

Quishing, a blend of "QR" and "phishing," is a rapidly evolving social engineering attack that leverages the widespread convenience and perceived trustworthiness of QR codes to deceive users into compromising their security. Cybercriminals create manipulated or fake QR codes that embed malicious links and when scanned, victims are unknowingly redirected to fraudulent and spoofed websites designed to steal sensitive information with seemingly legitimate webpages, such as fake login pages and credential harvesters, or to initiate malware downloads. Unlike direct malicious links, QR codes are often embedded as plain images within emails or attached documents, making them challenging for automated malware detectors and email filters to flag, thereby bypassing traditional email security filters and reaching the victim's inbox undetected.

Malicious QR codes are distributed through many channels, blurring physical and digital spaces; including emails, SMS messages, invoices, public posters, and product labels. Attackers use lures like discounts, urgent account verification, or security updates to prompt immediate action. In a financial context, fake bank communications instructing users to scan a QR code for "new data policies" could be sent out, leading to credential theft. In other instances, malicious QR codes could be embedded in stickers on public pay-to-park kiosks, redirecting victims to fraudulent payment sites. Quishing tactics are also used in spoofed bank statements or email receipts, with malicious QR codes redirecting users to phishing sites resembling official bank portals to steal login credentials. Fraud schemes impersonating prominent entities such as Microsoft, request users to scan QR codes for "voicemail access" or "**security updates**," often targeting corporate credentials and potentially bypassing MFA. The hybrid nature of Quishing necessitates broadening collaborative efforts beyond traditional sectors to include retail, hospitality, and municipal services, as these entities are often on the front lines of physical QR code deployment.

Executive Impersonation & Payment Fraud

Business Email Compromise (BEC) scams remained prevalent in 2024, with an emerging trend of criminals impersonating CEO's or suppliers to trick companies into making payments into their accounts. In a notable example, criminals hacked a CEO's email to send urgent payment requests to the finance department, while other reports indicate that the criminals could have intercepted invoices to change bank details. These attacks have become more tailored and personalised, creating a sense of urgency and legitimacy which could increase the likelihood of people falling victim to these scams.

Bank executive impersonation scams involving fake investment schemes have increasingly exploited popular communication platforms like Facebook and WhatsApp to reach potential victims. Scammers create fake profiles on these platforms or hijack legitimate ones to pose as

high-ranking officials from reputable financial institutions and initiate contact with individuals, often under the guise of offering exclusive investment opportunities. The use of familiar and trusted apps makes the approach feel more personal and credible, lowering the target's defences and increasing the likelihood of engagement.

These scams are particularly effective because they combine the perceived authority of financial executives with the accessibility and informality of social media and messaging apps. Victims may receive messages, voice notes, or even video calls that appear authentic, especially when enhanced by AI-generated content. The scammers often create a sense of urgency, pressuring individuals to act quickly before verifying the legitimacy of the offer. This blend of social engineering and digital impersonation makes platforms like Facebook and WhatsApp fertile ground for these fraudulent schemes.

Public "Loyalty Program" Scam

In the "loyalty program" scam, a fraudster, often in uniform, approaches victims with a tablet in public, offering to sign them up for a rewards program. They trick the victim into entering their bank card PIN or mobile banking login on the fraudster's device, which records the credentials and is used for fraudulent purposes.

Malware and Fake Banking Apps

In 2024, cybercriminals deployed advanced malware to compromise smartphones and PCs. A notable trend was the spread of trojan apps disguised as legitimate ones, such as a fake "DSTV Remote Update" app that installed banking trojans like "GoldDigger" or "Gigabud." This malware could monitor devices, capture banking login credentials, and surreptitiously approve transactions as some malware displayed overlay screens to capture details when a banking app was opened. On computers, phishing emails with attachments deployed keyloggers or remote access trojans. To protect against malware, users should only install apps from official app stores, keep devices updated, and use antivirus solutions.

SIM Swaps & Number Porting Fraud

SIM swap fraud continued to facilitate digital banking crimes and more specifically in the mobile banking (USSD) channel in 2024. A criminal convinces a mobile network to transfer a victim's cellphone number to a SIM card in the fraudster's possession. Once the victim's phone loses signal, the criminal receives all calls and SMS, including bank OTPs. SIM swaps were often used in combination with other tactics, like phishing for online banking passwords first, then performing a SIM swap to get the OTP for transfers. Customers are urged to contact their bank immediately if their phone suddenly shows "Emergency Calls Only," as this can indicate an unauthorized SIM swap.

Device Theft & Unauthorised Access

Criminals in South Africa have been stealing mobile phones in an attempt to access banking apps and login credentials as phones have been compared to bank cards due to the vast amount of information it contains. If a phone is unlocked or not securely protected, a thief can open banking or payment apps to transact. Even if locked, criminals may socially engineer access by sending phishing messages to trick the owner into revealing account credentials. Prevention tips include using strong PINs/biometrics, enabling remote wipe, never storing banking passwords in plaintext, and contacting your bank immediately if your phone is lost or stolen to deactivate banking access.

Money Mules & Laundering Networks

To avoid detection, criminals extensively used money mule accounts in 2024 to launder stolen funds. Scammers recruit individuals, who knowingly or unknowingly receive and pass on money through their own bank accounts. Syndicates also created fake or stolen ID accounts for this purpose. Stolen money is distributed in small amounts and funnelled through multiple mule accounts, sometimes across different banks. A notable trend was laundering via online betting accounts, where stolen funds are deposited into betting wallets and then "cashed out" as winnings to mask their origin. Cryptocurrency also remained a laundering tool. Banks and authorities intensified efforts to crack down on mule networks, with multiple arrests and improved monitoring.

"Long-Con" Romance & Investment Scams

2024 continued to see romance scams and "pig butchering" scams affecting bank customers. In romance scams, criminals cultivate online relationships over weeks, then manufacture emergencies to solicit funds via online banking. Pig butchering involves scammers gaining trust (not always romantically) and introducing fake investment opportunities, pressuring victims for larger investments before disappearing. These scams do not involve hacking but rely on victims willingly transferring money.

Each of the above modus operandi often overlaps with others and the banking industry tracks all these methods closely to adapt its prevention strategies.

Emerging Trends in 2024 and beyond

Several new or evolving trends shaped the digital banking crime landscape in 2024, providing insight into what we may face in 2025 and 2026:

AI-Powered Fraud (Deepfakes & Automation)

Criminals are leveraging artificial intelligence to enhance scams to make it seem more legitimate and convincing. Sophisticated AI-generated content was used to deceive victims, with error-free phishing emails and WhatsApp messages drafted by AI chatbots. Isolated reports of voice-based deepfake scams also emerged, where AI-cloned voices impersonated individuals. It can be expected that in 2025, criminals may use deepfake audio or video more often to impersonate bank officials or CEOs in real time. Banks are exploring countermeasures like AI-driven detection systems and training staff to establish verification protocols.

Fraud-as-a-Service & Collaboration Among Criminals

The use of Fraud-as-a-Service (FaaS) among underground markets grew during 2024, lowering the barrier to entry for cybercrime. Almost every aspect of a digital fraud operation can now be outsourced or bought, including phishing kits, malware rentals, and mule account networks. This means fraud syndicates do not need highly specialised and technical kills, leading to a broader base of attackers and faster spread of new scam techniques. To counter this, the banking industry and law enforcement are collaborating more closely to infiltrate and take down these criminal services.

Cryptocurrency in Fraud & Money Laundering

Cryptocurrency's role in digital banking crime grew in 2024 as more scams involved requesting payment in crypto, bypassing traditional banking systems and making tracing more difficult. After funds were stolen via conventional means, criminals often quickly converted a portion to cryptocurrency. This modus operandi is set to continue in 2025. This trend is prompting tighter regulations, with South African exchanges under stricter FIC obligations. Banks are also exploring blockchain analytics tools to trace stolen funds.

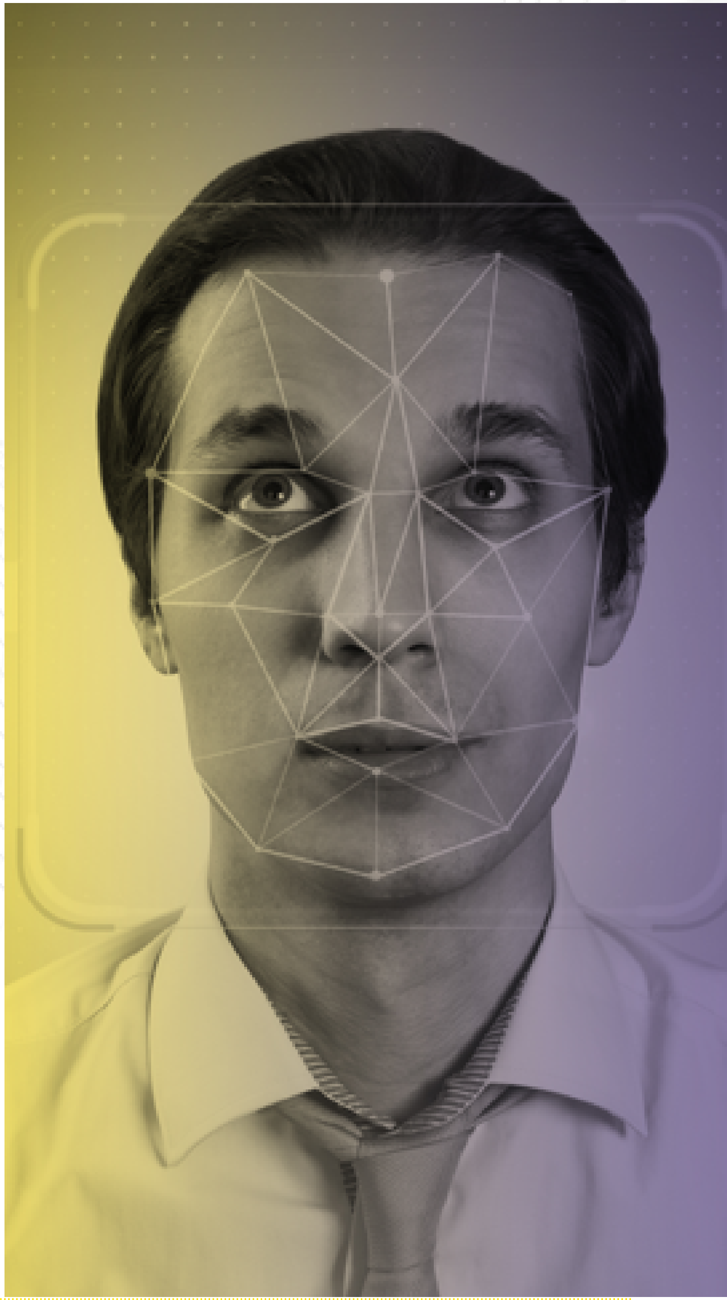
Targeting of Businesses & High-Net-Worth Individuals

Criminals also crafted highly targeted attacks against companies and wealthy individuals. This included Business Email Compromise (BEC) scams against businesses and bespoke cons against wealthy banking clients, often exploiting personal information gleaned from data breaches or social media. These tailored cons are high-effort, high-reward operations. Banks offer high-net-worth clients additional education and alert services, and advocate for measures such as dual authorization of payments for businesses.

Advanced Mobile Malware & Device Cloning

We anticipate that in 2025–2026, as more security features roll out, criminals will beef up their malware accordingly. 2024 already saw Android malware intercepting OTPs by abusing accessibility permissions. SIM cloning might also rise, where an attacker copies SIM data to create a duplicate, allowing OTP interception without triggering a SIM swap alert. Telecom providers are enhancing SIM card security. Malware targeting banking app communication is another worry. This highlights the importance of device security for customers: keeping phones/computers clean of malware is becoming as vital as keeping one's PIN secret.

These emerging trends paint a picture of an ever-evolving threat landscape. Criminals are innovating constantly, whether through technology like AI and malware or through inventive social tricks. However, banks and partners are also evolving in response, using better tech, stricter policies, and teamwork.



APPLICATION FRAUD

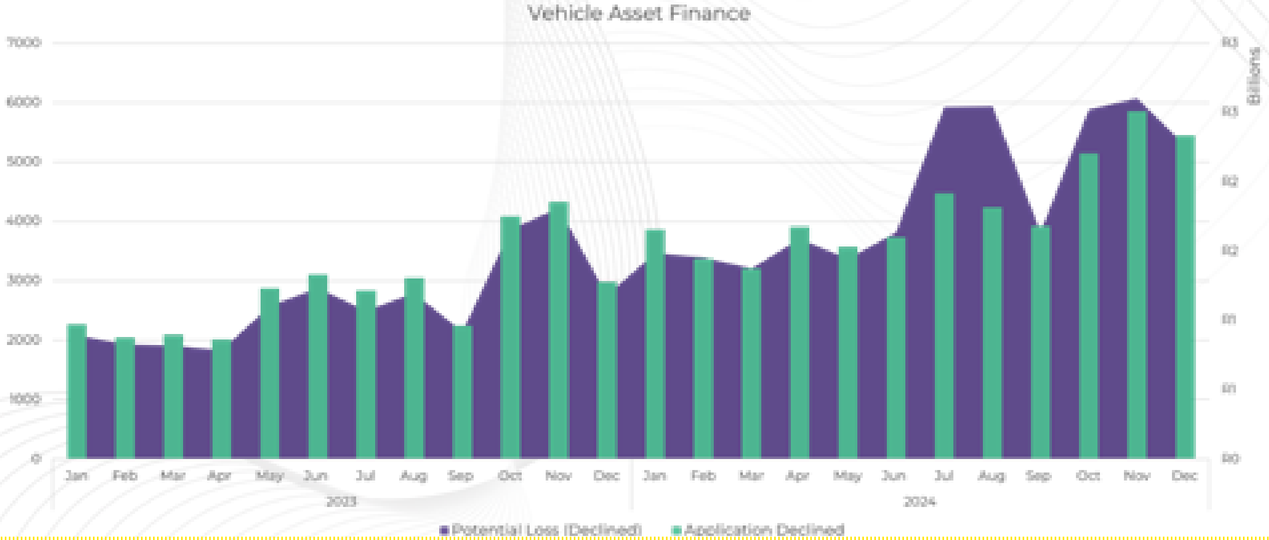
SECURED FRAUD (2023 & 2024)

Vehicle Asset Finance (VAF) Fraud

n 2024, there was a **49.6%** increase in fraudulent applications for Vehicle Asset Finance (VAF) with **50,765** reported incidents, compared to the previous year's **33,930** reported occurrences. The data indicates that potential losses also increased with **71.1%** from **R13.5 bn** in 2023 to **R23.0 bn** in 2024.

Product	2023	2024	Increase/ Decrease
Incidents	33 930	50 765	49.6% increase
Potential Loss	R 13,5 bn	R 23,0 bn	71.1% increase

Table 12: Vehicle Asset Finance 2023-2024



Nationally, more than half of the reported fraudulent applications in 2024 were concentrated in Gauteng and KwaZulu-Natal, with percentages of **39%** and **29%** respectively. This can mainly be attributed to Gauteng and KwaZulu-Natal being the most economically active provinces, with high volumes of vehicle transactions. This creates more opportunities for fraudsters to exploit:

- High demand for vehicle financing
- Greater anonymity in urban settings
- Larger pool of potential victims and institutions

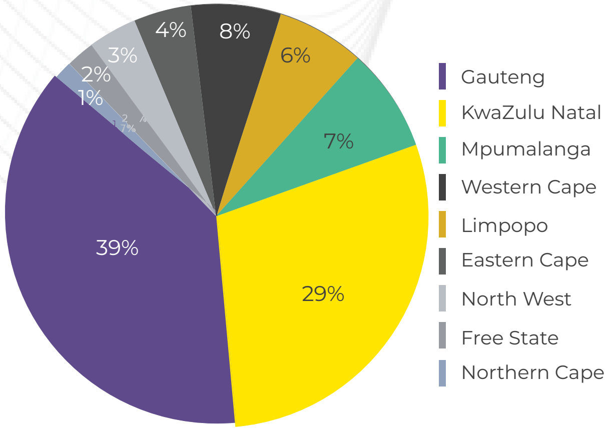


Figure 7: Vehicle Asset Finance 2023-2024 provincial

Prominent Modus Operandi

Cloned Motor Vehicles

The prominent Modus Operandi to commit VAF Fraud in South Africa are the Cloning of Motor Vehicles and the Illegal Change of Vehicle Ownership/Title. These modus operandi are identified through ongoing industry collaboration, case trend analysis, and shared insights from financial institutions and investigative partners.

A cloned motor vehicle is a stolen or hijacked vehicle that has been illegally registered using the details of a legitimate vehicle on the e-Natis system.

The vehicle is rapidly transferred between three or four individuals over short periods to obscure its origin, fabricate a legitimate ownership history, and hinder detection before being sold to unsuspecting buyers.

Illegal change of vehicle ownership involves fraudulently removing the bank as titleholder and re-registering the vehicle under another name, enabling it to circulate freely across borders or within South Africa without raising red flags, making it easier to sell to unsuspecting buyers.

International Perspective on VAF Fraud

Fraud attempts across the asset finance sector rose by **18%** globally in 2024 (Experian, 2024). This figure includes various lending categories such as equipment, commercial, and vehicle asset finance (VAF). While VAF is included in this increase, the growth is not solely attributable to vehicle-related fraud.

According to industry analysis, vehicle finance fraud losses reached **USD 9.2 bn** in 2024, an increase of more than **16%** year over year (BankInfoSecurity, 2024; AFSA-Online, 2024; Auto News, 2024). A large portion of this is linked to synthetic identity fraud, which now accounts for approximately **45%** of all auto-lending fraud, a sharp rise of **41%** compared to the previous year (AFSAOnline, 2024; AutoNews, 2024).

Synthetic identities are created by combining real and fictitious personal data, making them difficult to detect during credit application processes. These false identities are frequently used to obtain vehicle finance, with defaults typically occurring shortly after the vehicle is acquired (Experian, 2024).

The use of AI-generated documents and deepfakes further complicates detection. Fraudsters are increasingly submitting forged payslips, altered bank statements, and even impersonating applicants through AI-generated video and audio during remote verification (Nasdaq Verafin, 2024).

In addition, cross-border fraud syndicates continue to pose a global threat. These organised networks often transport financed vehicles across international borders before defaults are detected, especially in regions where border controls or recovery frameworks are weak. While specific routes vary, this trend is frequently observed in parts of Eastern Europe, Africa, and Asia (OCCRP, 2024). These schemes often involve insider collusion or third-party “mules”, significantly complicating recovery and contributing to higher institutional losses.

References

Experian (2024): Global Fraud Trends Report

Nasdaq Verafin (2024): Global Financial Crime Report

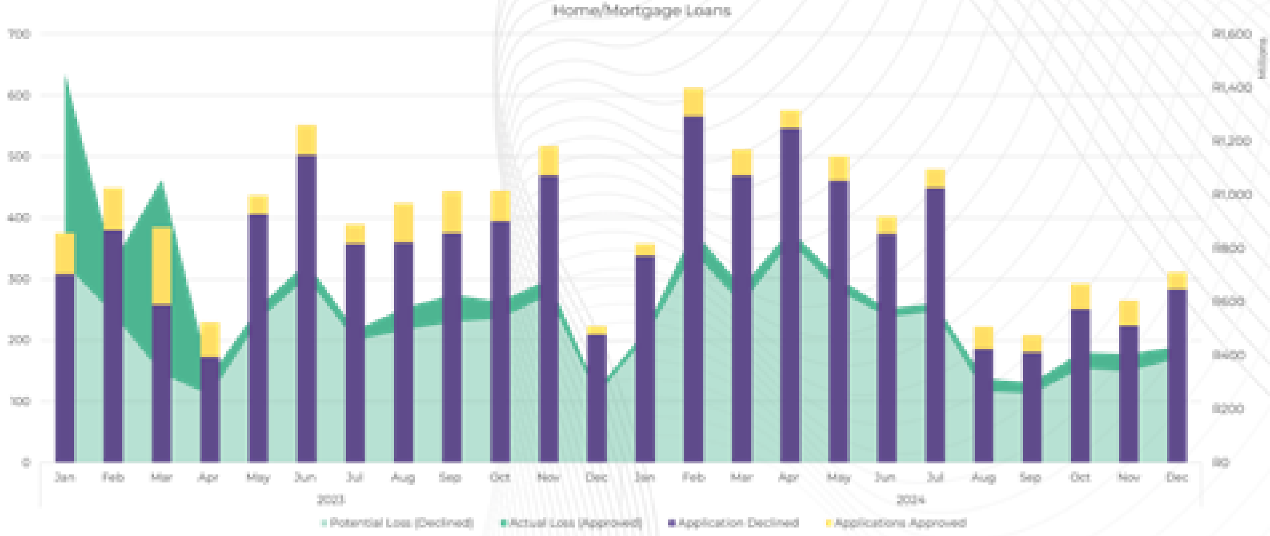
OCCRP (2024): Financial Crime Losses

BankInfoSecurity (2024), AFSAOnline (2024), AutoNews (2024) – Industry estimates referenced in publicly available fraud trend analysis

Home and Mortgage Loan Fraud

Product	2023	2024	Increase / Decrease
Incidents	4 867	4 739	-2.6% decrease
Potential Loss	R 5,9 bn	R 6,0 bn	0.5% increase
Actual Loss	R 2.1 bn	R 575,7 m	-73.3% decrease

Table 13: Home and mortgage loan fraud



Fraudulent applications for home and mortgage loans declined by **2.6%**, dropping from **4,867** cases in 2023 to **4,739** in 2024. Only **9%** of the reported fraudulent applications were successful in 2024.

The potential loss due to these fraudulent applications grew by **0.5%**, with losses amounting to **R5,9 bn** in 2023 and **R6.0 bn** in 2024. The actual loss decreased by **73.3%**, from **R2.1 bn** to **R575.7 m** in 2023. This loss is mitigated by the fact that the property still belongs to the bank. However, even though the banks have certain safeguards such as bonds and property deed registration in place in most cases of successful fraudulent applications; they still face significant expenses related to legal proceedings and eviction processes.

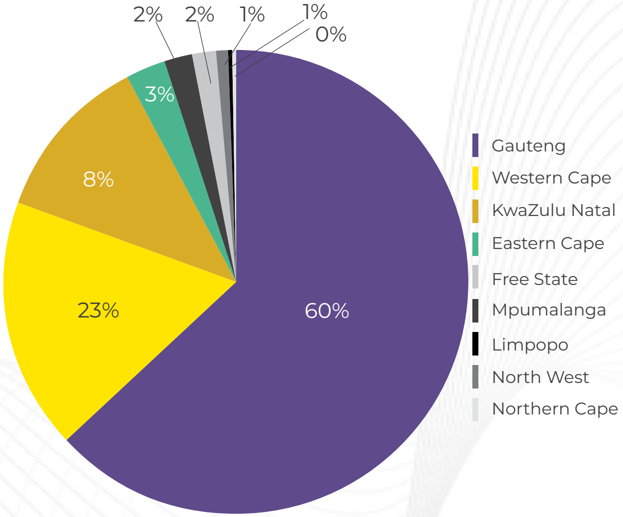


Figure 8: Home and mortgage loan fraud provincial

In 2024, Gauteng and the Western Cape emerged as the leading provinces for home loan application fraud, accounting for **60%** and **23%** of reported cases respectively. This trend is largely attributed to the high population density and economic activity concentrated in these regions, which naturally results in a greater volume of loan applications. Additionally, elevated property values in these provinces create a more lucrative environment for fraudsters, who are incentivised to target high-value markets where the potential financial gain is significantly higher.

Prominent Modus Operandi

Ongoing industry collaboration, case trend analysis, and shared insights from financial institutions and investigative partners indicated that home loan fraud occur in various forms, including but not limited to the following:

- Misrepresentation of application details that have been identified as the most prevalent method of fraud. This refers to the deliberate falsification, alteration, or omission of information provided on loan applications to deceive lenders and to gain approval. One such prominent form of misrepresentation identified is income fraud, where individuals falsify or inflate income information to meet lender requirements or qualify for larger loan amounts. This is particularly evident when discrepancies are found in the income stated on pay slips.
- Another significant concern in this area is Credit Profile Building, which involves unlawful and deceptive practices used to artificially enhance creditworthiness or create a misleading impression of financial stability. Individuals or entities often transfer funds into and out of an account over an extended period without a valid reason, solely to generate turnover. This activity aims to simulate a legitimate salary or income, even though the applicant or company did not genuinely earn that income. The goal is to present the person or company as authentic and creditworthy. Syndicates frequently employ this modus operandi, utilizing both South African and non-South African citizens and companies to establish creditworthy profiles. This form of fraud, which can be described as going from “zero to hero,” ranks as the third-highest reported type of fraudulent activity and is used across all platforms of application fraud.

International Perspective on home loan fraud

Between 2023 and 2024, home loan application fraud showed a notable increase, particularly in the United States. According to CoreLogic, the Mortgage Application Fraud Risk Index rose by **8.3%** year-over-year, with approximately **1** in every **123** applications exhibiting signs of fraud in Q2 2024 (CoreLogic, 2024). This trend mirrors broader global financial crime patterns, where fraud-related losses reached an estimated **$485.6 bn** in 2023 (Nasdaq Verafin, 2024).

A significant contributor to this rise is synthetic identity fraud. Fraudsters construct convincing borrower profiles by blending real and fabricated personal data. These identities are often used to apply for home loans, supported by falsified income or employment documentation. Their sophistication makes it difficult to detect using traditional verification methods (Experian, 2024).

In 2024, the threat landscape intensified with the use of AI-generated documents and deepfakes. Fraudsters now leverage generative AI to produce authentic-looking payslips, bank statements, and even video or voice deepfakes to impersonate applicants during remote onboarding. This has made fraud detection more complex and resource-intensive (Experian, 2024).

Additionally, cross-border fraud syndicates have been implicated in mortgage fraud schemes. These networks exploit jurisdictional gaps and regulatory inconsistencies to submit fraudulent applications across multiple regions. Often using mules or shell companies to obscure ownership and intent, these schemes significantly complicate recovery and increase institutional losses (Experian, 2024; Nasdaq Verafin, 2024).

References

CoreLogic (2024) Mortgage Fraud Risk Up 8.3% From Last Year. Available at: https://nationalmortgageprofessional.com/news/mortgage-fraud-risk-83-last-year

Experian (2024) Global Identity & Fraud Report 2024. Available at: https://www.experian.com/blogs/global-insights/wp-content/uploads/2024/11/Global_Fraud_Trends_Report_2024_FinalV.pdf

Nasdaq Verafin (2024) 2024 Global Financial Crime Report. Available at: https://www.nasdaq.com/global-financial-crime-report

UNSECURED FRAUD (2023 & 2024)

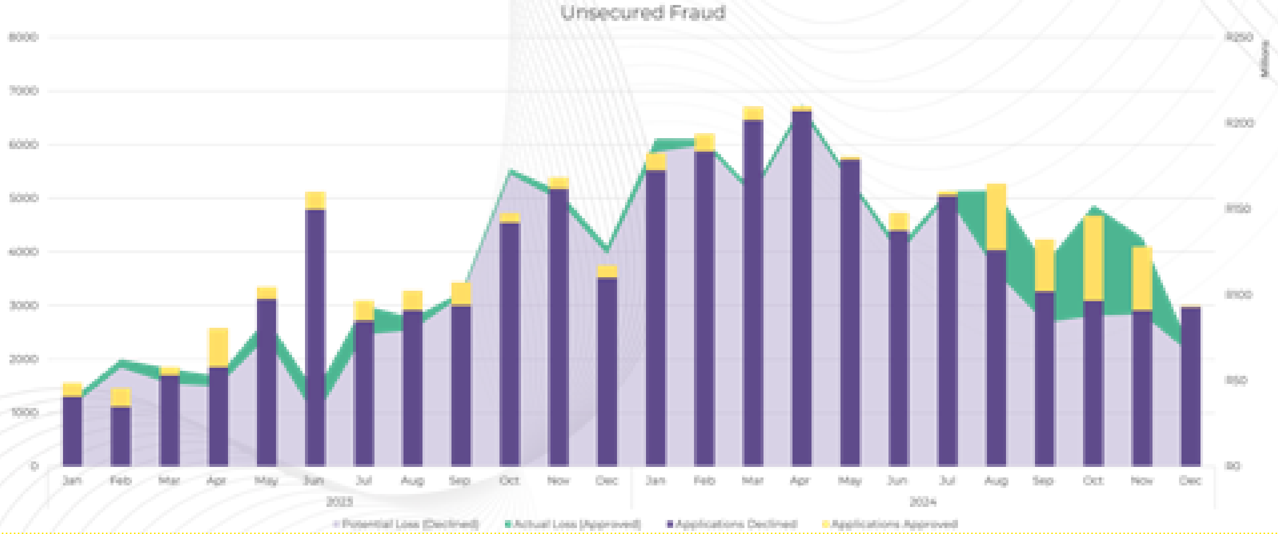
Product	2023	2024	Increase / Decrease
Incidents	39 570	62 346	57.6% increase
Potential Loss	R 997,1 m	R 1.6 bn	62.4% increase
Actual Loss	R 87,9 m	R 221.7 m	>100% increase

Table 14: Unscure fraud 2023-2024

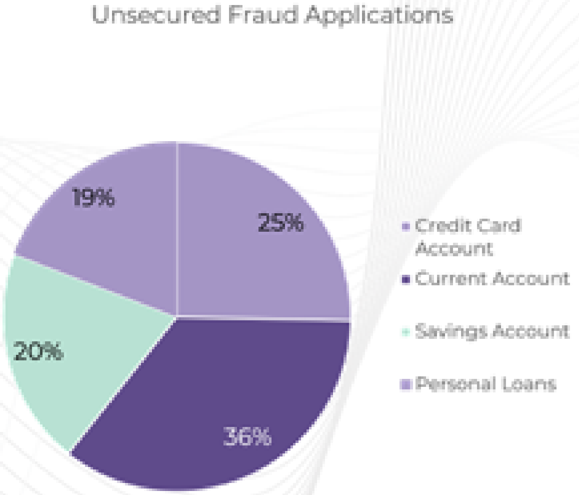
Unsecured fraud refers to fraudulent schemes involving credit products that do not require collateral, such as credit cards, bank accounts (current and savings accounts), and personal loans.

In 2023, unsecured fraud applications reported to SABRIC rose by **57.6%** with **62 346** occurrences in comparison to the previous year's **39 570** occurrences.

The potential loss also increased by **62.4%** from **R997.1 m** in 2022 to **R1.6 bn** in 2024, while the actual loss increased with more than **100%** from **R87.9 m** in 2023 to **R221.7 m** in 2024. A significant **90%** of the reported applications in 2024 were flagged as fraudulent and was subsequently declined.



During 2023, the largest portion, comprising of **36%,** of fraudulent applications on accounts was associated with Current Accounts, while Credit Card Accounts represented **25%**, and Saving Accounts as well as Personal Loans made up a smaller proportion of **20%** and **19%** respectively.



In 2023, Gauteng experienced the highest percentage of fraud cases at **68%** being one of the provinces with a high concentration in population density and economic activity which naturally results in a greater volume of loan applications, followed by the Western Cape at **9%** and KwaZulu-Natal at **8%.**

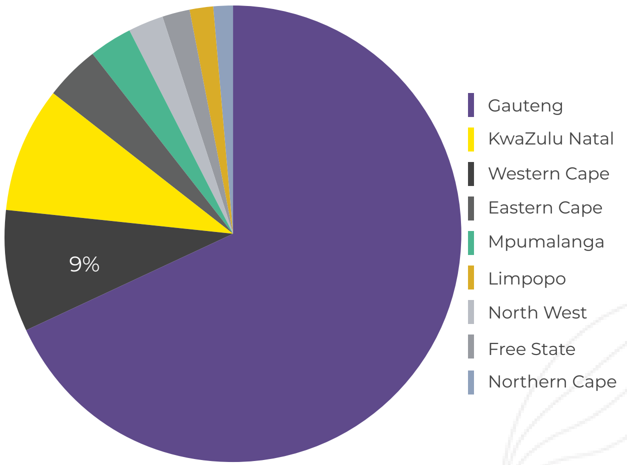


Figure 10: Unsecured fraud provincial

Prominent Modus Operandi

Insights from industry collaboration: case trend analysis indicated that using of Mule Accounts in application fraud is quite prevalent especially in the Unsecured fraud space where cash can be easily obtained and transferred quickly into other accounts. One such method is where fraudster funnel illicit funds. Fraudsters use mule accounts to receive and transfer money obtained through fraudulent loan applications. Once the loan is approved and disbursed, the funds are quickly moved through one or more mule accounts to make tracking difficult and to obscure the money trail. Fraudsters may create synthetic identities (combinations of real and fake information) to open mule accounts. These accounts are then used to apply for loans or credit, with the ultimate goal of defaulting and laundering the loan proceeds through other mule accounts.

International Persective Unsecured Fraud

Unsecured fraud targeting products such as credit cards, current accounts, savings accounts, and personal loans saw a sharp increase in 2024. This rise has been driven by economic pressure, identity theft, and increasingly sophisticated fraud tactics.

TransUnion reported that **13.5%** of all new online accounts created in 2023 were flagged as potentially fraudulent (TransUnion, 2024). One of the most concerning developments is the surge in first-party fraud. In these cases, individuals use their real identities but submit false information, such as fake income or employment details. This type of fraud accounted for **36** percent of all attacks in 2024, up from 15 percent the year before (LexisNexis Risk Solutions, 2025).

The sections below outline how these types of fraud are affecting different financial products.

Credit Card Fraud

Credit card application fraud remains one of the most common forms of identity fraud. In the United States, more than **416,000** incidents were reported in 2023, making up around **40%** of all identity theft cases (FTC, 2024). The United Kingdom also saw a significant increase, with impersonation fraud involving store cards rising by **59%** in the first half of 2024 (Cifas, 2024).

Fraudsters use stolen personal data to apply for credit cards in someone else's name. They also create synthetic identities by combining real and fake information, allowing them to build credit histories and apply for cards without detection. In first-party fraud, individuals use their own identity but provide false details, such as inflated income, with no intention of repaying the debt.

Current Account Fraud

Fraudulent applications for current accounts are often used to enable other crimes, including money laundering and cheque fraud. In the UK, these cases increased by 19 percent in the first half of 2024 compared to the same period in 2023 (Cifas, 2024). In contrast, figures in the United States declined, likely due to stronger identity verification procedures (FTC, 2024).

Criminals may impersonate real individuals using forged documents or stolen data. Others recruit people to open accounts under their own names, which are then used to move illicit funds. Some individuals open accounts specifically to misuse them, such as writing bad cheques or exploiting overdraft facilities. More than **37,000** such cases were recorded in the UK in early 2024.

Savings Account Fraud

Savings account fraud is less frequently reported as a standalone category but remains a serious concern. These accounts are often used to temporarily hold stolen or illegally obtained funds. Because savings accounts typically involve larger balances and fewer transactions, they may attract less scrutiny, making them useful for money laundering and other financial crimes.

Fraudsters use stolen or fabricated personal details to open these accounts. In some cases, individuals misuse savings accounts by depositing counterfeit cheques or opening multiple accounts under slightly varied identities to exploit bank promotions.

Personal Loan Fraud

Personal loan fraud saw the most dramatic increase in 2024. In the UK, fraudulent applications more than doubled, rising by **109%** in the first half of the year (Cifas, 2024). The United States reported over **81,000** cases of loan-related fraud in 2023, with indications that the trend continued into 2024 (FTC, 2024). This surge is largely attributed to financial stress caused by inflation and the rising cost of living.

Criminals use stolen or synthetic identities to secure loans they do not intend to repay. First-party misrepresentation is also common, where individuals provide false information about their income or employment. Some schemes involve collusion between multiple individuals or even insiders within financial institutions who approve fraudulent loans. Organized fraud rings use bots and shared databases of stolen identities to submit large volumes of applications across multiple lenders, taking advantage of weak verification systems.

Impact and Response

Each successful fraudulent loan represents a direct financial loss to the lender, typically ranging from five thousand to fifteen thousand dollars per case. When scaled across thousands of incidents, these losses can reach hundreds of millions annually.

To combat this, financial institutions are strengthening their fraud prevention efforts. Measures include biometric and video-based identity checks, device fingerprinting, IP monitoring, and cross-institution fraud reporting. Advanced analytics and machine learning are also being used to detect suspicious patterns.

The rise in first-party fraud is prompting lenders to rethink how they assess risk. Many are moving beyond basic identity checks to verify the accuracy and consistency of the information provided in loan and credit applications.

References

Cifas. (2024) Cifas intelligence shows frauds are becoming more complex and sophisticated (Press Release, 13 August 2024). Cifas, London.

Federal Trade Commission (FTC). (2024) Consumer Sentinel Network Data Book 2023. FTC, Washington, DC.

LexisNexis Risk Solutions. (2025) Cybercrime Report 2024 (Annual fraud analysis report). LexisNexis, Atlanta, GA.

The Nilson Report. (2023) Global Payment Card Fraud Losses (2022 Data). The Nilson Report, Carpinteria, CA.

TransUnion. (2024) 2024 State of Omnichannel Fraud Report (Press Release, 21 March 2024). TransUnion, Chicago, IL.

CARD FRAUD

FINANCIAL CRIME OVERVIEW: CREDIT & DEBIT (2023 & 2024)

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

Product	2023	2024	Change
Gross Fraud (credit & debit)	R1 161 524 026	R1 466 231 292	26.2% increase
Credit	R446 048 901	R559 338 787	25.4% increase
Debit	R715 475 126	R906 892 505	26.7% increase

Total gross fraud losses for South African issued cards increased by **26.2%** from 2023 **(R1.1bn)** to 2024 **(R1.4bn)**. Gross fraud losses on South African issued credit cards specifically amounted to **R559.3m** in 2024, an increase of **25.4%** compared to 2023 **(R446.0m)**.

Gross fraud losses on South African issued debit cards amounted to **R906.8m** in 2024, a **26.7%** increase compared to 2023 **(R715.4m)**. Similar to 2023 debit card remained the card type with the highest fraud amount in 2024.

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

Product	2023	2024	Change
Gross Fraud (credit & debit)	R479 114 149	R573 151 196	19.6% increase
Credit	R174 122 812	R186 128 164	6.8% increase
Debit	R304 991 337	R387 023 032	26.9% increase

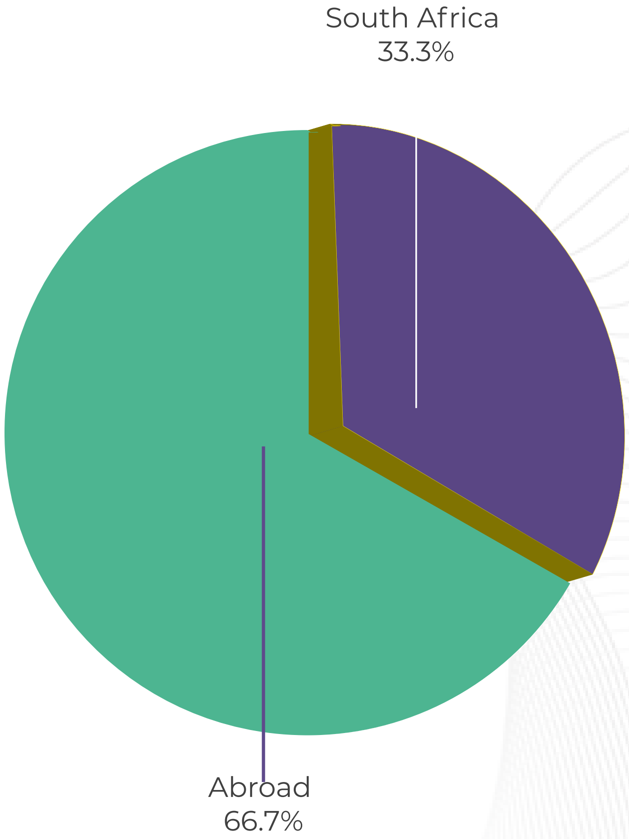
In 2024, gross fraud losses on South African issued cards due to fraudulent transactions within South Africa rose by **19.6%**, reaching **R573.1 million** compared to **R479.1m** in 2023.

Credit card fraud increased by **6.8%** in 2024 **(R186.1m)** compared to 2023 **(R174.1m)**. Debit card fraud increased by **26.9%**, comparing 2024 **(R387.0m)** to 2023 **(R387.0m)**.

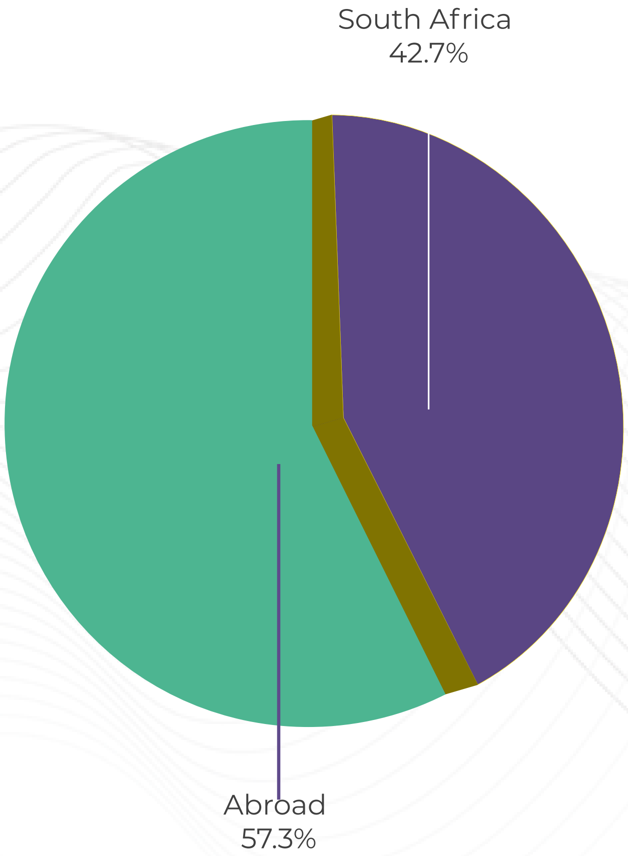
In 2024, Card Not Present (CNP) **(52%)** and Lost and/or Stolen **(36%)** contributed to most of the fraud in South Africa.

South Africa VS Abroad

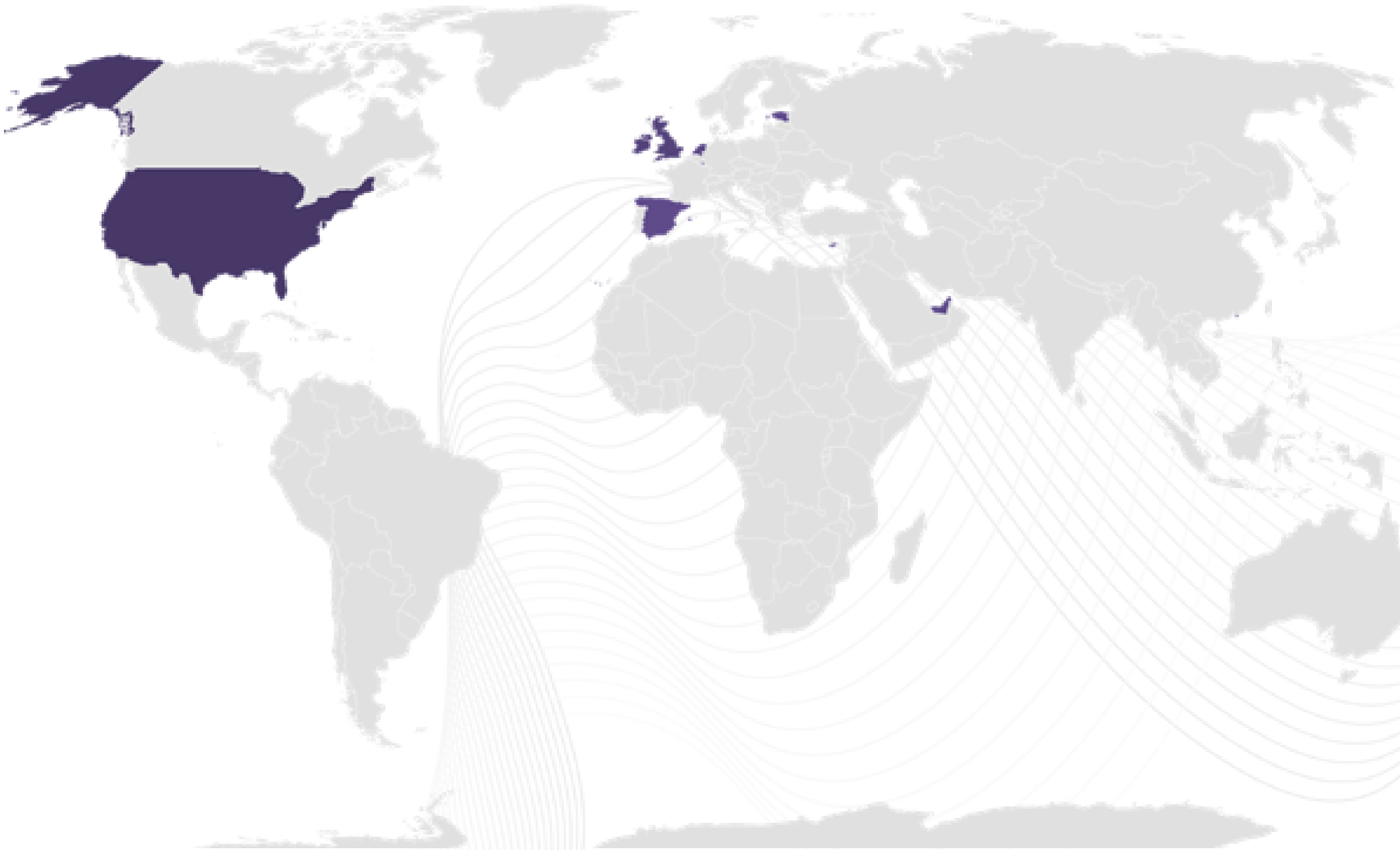
Credit Card



Debit Card



A significant proportion of card fraud involving South African issued cards occurred abroad. Specifically, **66.7%** of credit card fraud and **57.3%** of debit card fraud took place outside South Africa.



United States

Ireland

United Kingdom

Netherlands

Cyprus

United Arab Emirates

Hong Kong

Luxembourg

Spain

Estonia

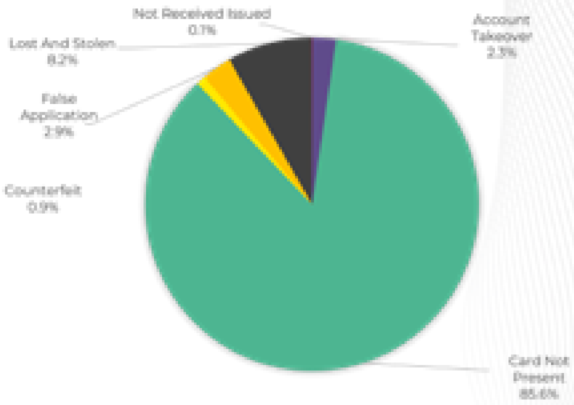
Figure 13: This map highlights the leading countries where fraudulent transactions involving South African-issued credit and debit cards have been reported.

Fraud Types: All Countries - 2024

Credit	Rand Values	Debit	Rand Values
Account Takeover	R11.2m	Account Takeover	R1.6m
Card Not Present	R416.6m	Card Not Present	R583.7m
Counterfeit	R4.4m	Counterfeit	R18.6m
False Application	R14.1m	False Application	R7.8m
Lost and/or Stolen	R39.9m	Lost and/or Stolen	R252.2m
Not Received Issued	R301.8k	Not Received Issued	R1.4m

Table 17: Fraud Types: All Countries - 2024

Credit Card



In 2024 Card Not Present (CNP) fraud contributed to **85.6%** of gross fraud losses on South African issued credit cards, followed by Lost and/or Stolen **(8.2%)** and False Applications **(2.9%)**.

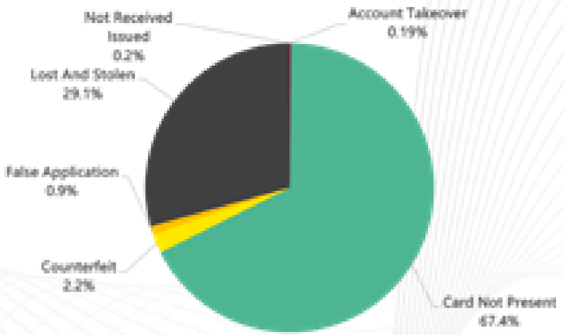
CNP fraud **(R416.6m)** increased by **19.5%** compared to 2023. Lost and/or Stolen fraud **(R39.9m)** decreased with **20%** compared to 2023 **(R49.8m)**.

CNP continued to be the fraud type that accounted for the largest portion of fraud. In 2024, the banking industry continued to report phishing and OTP vishing as prominent scams, mirroring trends from previous years. In these schemes, unsuspecting clients were deceived by way of social engineering techniques into providing their banking details to fraudsters.

Internationally, trends similar to those observed in South Africa have been reported. According to the UK Finance Half Year Fraud Report 2024, fraudsters are increasingly exploiting stolen card details through phishing, malware, and data breaches. These attacks often target consumers via social media platforms and fraudulent online merchants, highlighting the evolving nature of digital fraud threats.

https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/half-year-fraud-update-2024

Debit Card



In 2024, CNP fraud with a debit card contributed to **67.4%**, followed by Lost and Stolen **(29.1%)** and Counterfeit **(2.2%)**.

Card Not Present fraud totalled **R583.7m** in 2024, marking a **32.9%** increase compared to 2023 **(R439.1m)**. The continuous popularity of e-commerce has led to increased use of debit cards for online purchases, thereby expanding the risk landscape for CNP-related fraud.

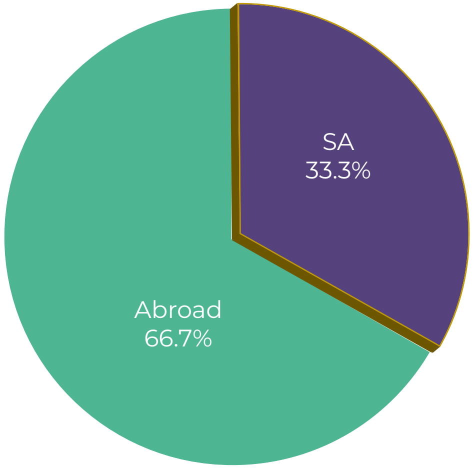
Lost and/or Stolen card fraud amounted to **R252.2m**, reflecting a **12.4%** increase compared to 2023 **(R224.5m)**. Key contributors to this fraud category, involving card theft or swopping at ATMs, remained prevalent throughout 2024.

Card Not Present (CNP)

Product	2023	2024	Inc/Dec	Card Not Present as % of Gross Fraud Loss
Credit	R348 709 260	R416 605 299	19.5% increase	74.5%
Debit	R439 198 436	R583 742 849	32.9% increase	64.4%

Table 18: Card Not Present (CNP)

Credit Card 2024



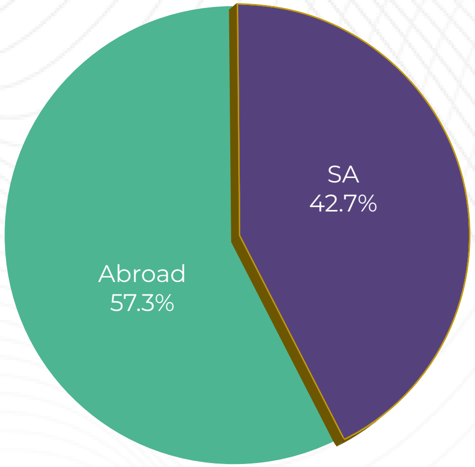
In 2024 **66.7%** of CNP credit card fraud occurred abroad.

Prominent merchant groups were:

- Advertising Services
- Travel Agencies
- Betting
- Clothing Stores
- Security Brokers

Advertising Services contributed to **16%** of the reported fraud.

Debit Card 2024



In 2024 **57.3%** of CNP debit card fraud occurred abroad.

Prominent merchant groups were:

- Electronic Sales
- Digital Goods
- Advertising Services
- Professional Services
- Computer Software

Social engineering tactics such as smishing and vishing continued to be a prominent modus operandi throughout 2024. Fraudsters successfully acquired sufficient personal information to link clients' cards to virtual wallets, subsequently obtaining electronic authorisation or one-time passwords (OTPs) from clients to facilitate fraudulent transactions.

The Australian Payments Network reported in their annual Australian Payment Fraud Report 2024 that CNP fraud accounted for over **90%** of all card fraud in 2023, with a notable surge in overseas CNP fraud, which now surpasses domestic levels.

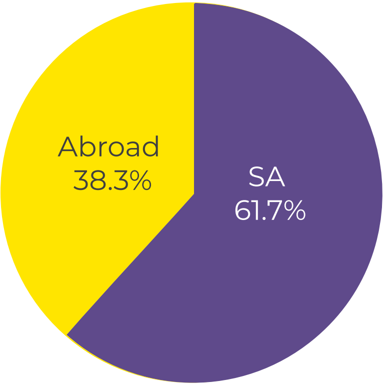
(https://www.auspaynet.com.au/resources/reports)

Lost and/or Stolen

Product	2023	2024	Inc/Dec	Lost and/or Stolen as % of Gross Fraud Loss
Credit	R49 889 893	R39 926 217	20.0% decrease	7.1%
Debit	R224 561 290	R252 294 656	12.4% increase	27.8%

Table 19: Lost and/or Stolen

Credit Card 2024



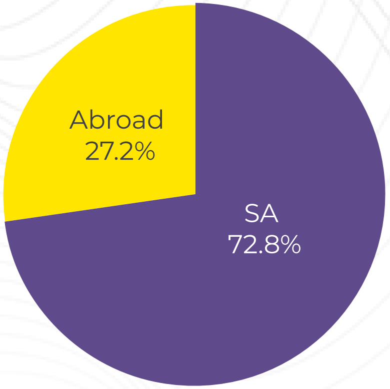
In 2024 **61.7%** of Lost and/or Stolen credit card fraud occurred in South Africa.

Prominent merchant groups were:

- ATMs
- Advertising Services
- Supermarkets
- Toll Plazas
- Drinking Places

10.9% of the gross fraud losses on Lost and/or Stolen cards occurred at ATMs.

Debit Card 2024



In 2024 **72.8%** of Lost and/or Stolen debit card fraud occurred in South Africa.

Prominent merchant groups were:

- ATMs
- Toll Plazas
- Supermarkets
- Liquor Stores
- Drinking Places

Of the total gross fraud losses involving Lost and/or Stolen debit cards, **26.6%** resulted from ATM withdrawals, while **15.2%** occurred at tollgates.

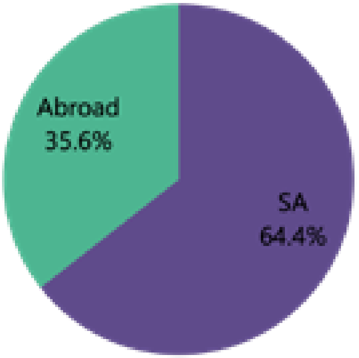
Card swopping/theft at ATMs remained a prevalent method of debit card fraud in South Africa during 2024. Fraudsters operate in groups near ATMs, targeting individuals during transactions. They distract victims, often under the guise of offering assistance, and then steal the victim's card. Once the card is in their possession, fraudsters use a PIN they have observed through shoulder surfing to withdraw funds.

Counterfeit

Product	2023	2024	Inc/Dec	False App as % of Gross Fraud Loss
Credit	R9 544 148	R4 441 673	53.5% decrease	0.8%
Debit	R12 664 460	R18 661 496	47.4% increase	2.1%

Table 20: Counterfeit

Credit Card 2024

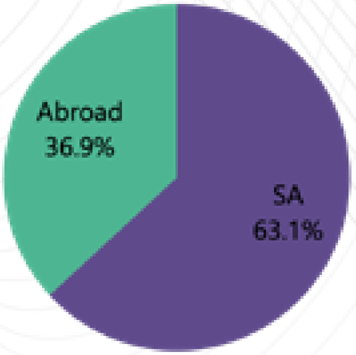


In 2024 **64.4%** of Counterfeit credit card fraud occurred in South Africa.

Prominent merchant groups were:

- Toll Plazas
- Personal Services
- Service Stations
- Supermarkets
- Miscellaneous Food Stores
- **11.8%** of the gross fraud losses on Counterfeit credit cards occurred at Toll Plazas.

Debit Card 2024



In 2024 **63.1%** of Counterfeit debit card fraud occurred in South Africa.

Prominent merchant groups were:

- Service Stations
- ATMs
- Supermarkets
- Toll Plazas
- Advertising Services

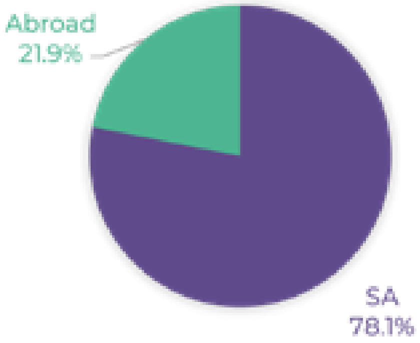
Service Stations contributed **11.9%** of the gross fraud losses on Counterfeit debit cards.

False Application

Product	2023	2024	Inc/Dec	False App as % of Gross Fraud Loss
Credit	R27 434 295	R14 194 243	48.3% decrease	2.5%
Debit	R2 933 077	R7 874 800	+100% increase	0.9%

Table 21: False application

Credit Card 2024



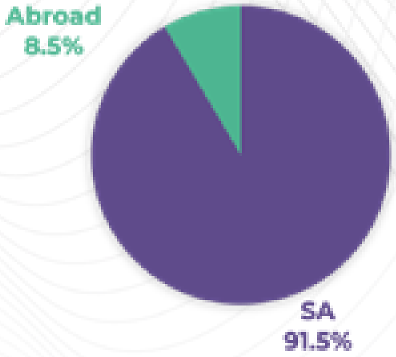
In 2024 credit card fraud with a False Application **(78.1%)** occurred in South Africa.

Prominent merchant groups were:

- ATMs
- Meat Provisioners
- Manual Cash Disbursements
- Supermarkets
- Computers

22.7% of the gross fraud losses on False Application credit cards occurred at ATMs.

Debit Card 2024



In 2024 debit card fraud with a False Application **(91.5%)** occurred in South Africa.

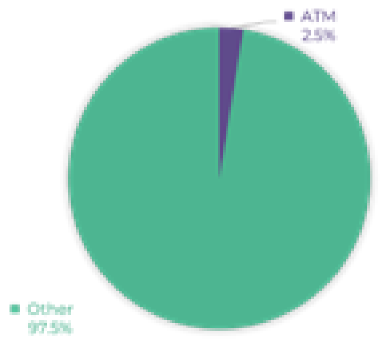
Prominent merchant groups were:

- ATMs
- Supermarkets
- Direct Marketing
- Liquor Stores
- Advertising Services

70.8% off the gross fraud losses on False Application debit cards were ATM withdrawals.

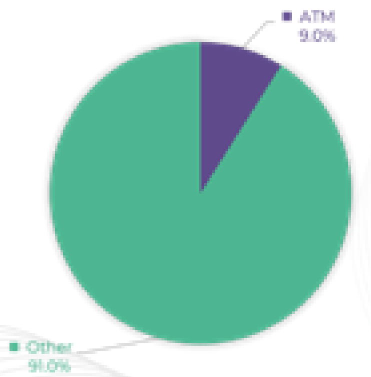
Card Fraud: ATM vs. Point of Sale (POS)

Credit: Rand Value



Transactions at POS devices contributed to **97.5%** of credit card fraud when compared to ATM withdrawals **(R12.9m)**.

Debit: Rand Value



Debit card fraud at ATMs **(R81.4m)** contributed to **9.0%** of gross fraud losses when compared to POS **(91.0%)** transactions.

International Perspective

Credit Card

Card Not Present, Lost and/or Stolen and Counterfeit fraud were prominent in the countries detailed below.

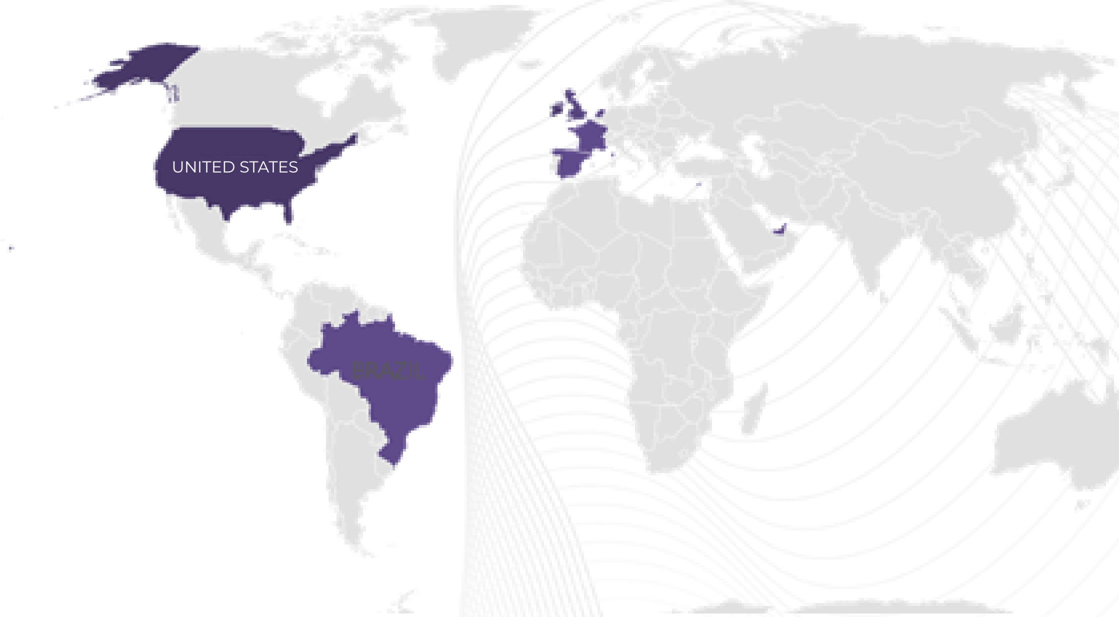


Figure 23: World map international perspective

This table highlights the leading countries where fraudulent transactions involving South African-issued credit cards have been reported.

Card Not Present (CNP)	Lost and/or Stolen (L&S)	Counterfeit (CTF)
UNITED STATES	UNITED STATES	UNITED KINGDOM
IRELAND	IRELAND	UNITED STATES
UNITED KINGDOM	UNITED KINGDOM	IRELAND
NETHERLANDS	NETHERLANDS	UNITED ARAB EMIRATES
UNITED ARAB EMIRATES	SPAIN	SPAIN
BRAZIL	BRAZIL	THAILAND
CYPRUS	ITALY	NETHERLANDS
FRANCE	UNITED ARAB EMIRATES	MEXICO
HONG KONG	LUXEMBOURG	POLAND
SPAIN	GERMANY	ESTONIA

Debit Card

Card Not Present, Lost and/or Stolen, and Counterfeit fraud were prominent in the countries reflected below.

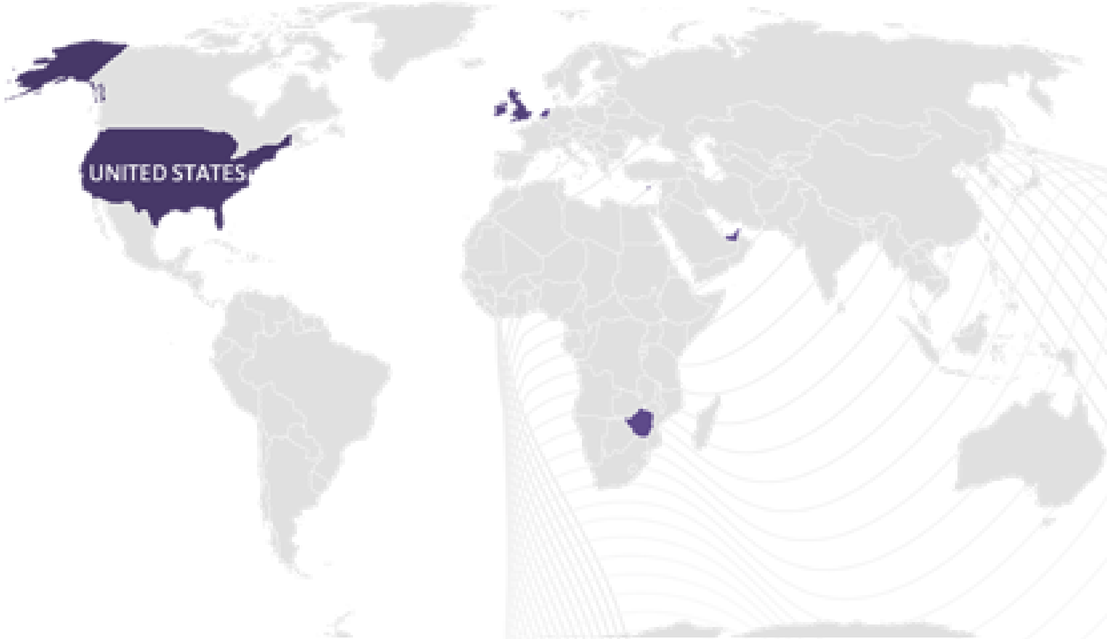


Figure 24: World map Debit Card

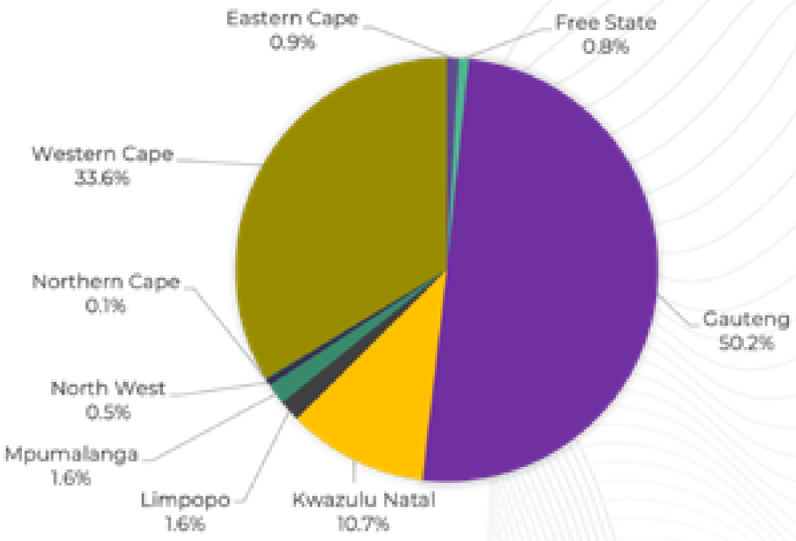
This table highlights the leading countries where fraudulent transactions involving South African issued debit cards have been reported.

Card Not Present (CNP)	Lost and/or Stolen (L&S)	Counterfeit (CTF)
UNITED STATES	UNITED STATES	UNITED STATES
UNITED KINGDOM	UNITED KINGDOM	IRELAND
IRELAND	IRELAND	UNITED KINGDOM
CYPRUS	KOREA REPUBLIC OF	UNITED ARAB EMIRATES
NETHERLANDS	NETHERLANDS	NETHERLANDS
LUXEMBOURG	LUXEMBOURG	MOZAMBIQUE
HONG KONG	CYPRUS	INDONESIA
MALTA	CANADA	CANADA
VIETNAM	UNITED ARAB EMIRATES	ZAMBIA
SPAIN	AUSTRALIA	LUXEMBOURG

Provincial Overview

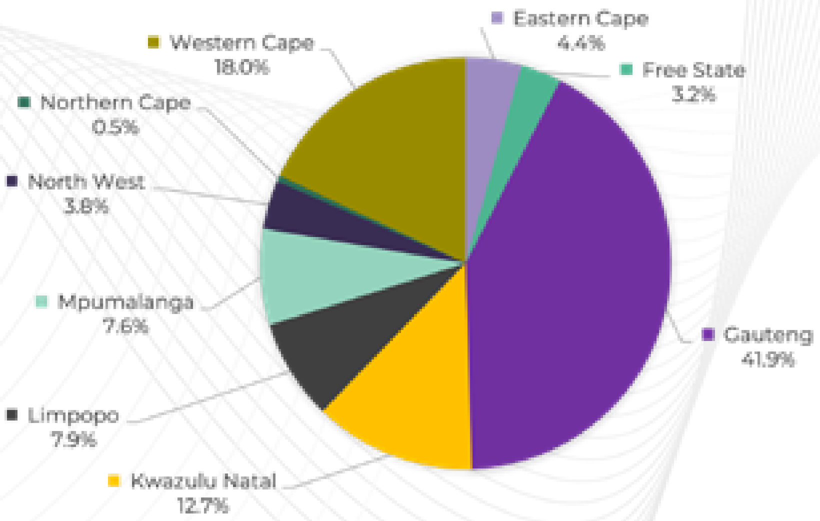
Credit Card – Rand Value

In 2024, Gauteng experienced the highest incidence of credit card fraud, accounting for **50.2%** of reported cases, followed by the Western Cape at **33.6%** and KwaZulu-Natal at **10.7%**. The most prevalent fraud types involving credit cards were Card Not Present **(72.1%)**, Lost and/or Stolen **(14%)**, and False Application **(6.32%)**.



Debit Card – Rand Value

In 2024, Gauteng **(41.9%)**, Western Cape **(18%)**, and KwaZulu-Natal **(12.7%)** emerged as the top three provinces affected by debit card fraud. The majority of fraudulent transactions involved Lost and/or Stolen debit cards **(48.5%)**, followed by Card Not Present fraud **(45.4%)**.



CONCLUSION

The 2024 crime statistics reflect the dynamic and rapidly evolving nature of financial crime in South Africa. While the industry has made commendable progress in reducing certain contact crimes, such as associated robberies and ATM attacks, the exponential rise in digital and application fraud highlights the growing sophistication of criminal syndicates.

SABRIC recognises that as fraudsters continue to innovate, the financial services sector must also do so. The emergence of artificial intelligence as both a tool for criminals and a defence mechanism for institutions highlights the ambivalent role of technology. Combating such threats requires not only advanced technological interventions but also strengthened human vigilance, robust internal controls, and industry-wide collaboration.

The successes recorded in 2024 were made possible by the unwavering commitment of SABRIC members, law enforcement agencies, and our partners across the public and private sectors. Through strategic information sharing, targeted interventions, and a shared sense of purpose, the industry continues to build resilience against criminal activity.

Looking ahead, SABRIC remains committed to its purpose of enabling a safe banking environment through innovation, partnership, and proactive intelligence. As financial crime becomes more complex, so must our response, aimed to be driven by unity, foresight, and the collective will to protect the integrity of South Africa's financial system. Together, through collaboration and adaptability, we will continue to anticipate emerging threats, reduce vulnerabilities, and strengthen the banking ecosystem for all.