ANNUAL CRIME STATISTICS 2025

SABRIC | South African Banking Risk Information Centre

CONTENTS

EXECUTIVE SUMMARY

The 2025 SABRIC Annual Crime Statistics Report highlights the changing nature of banking crime in South Africa and the continued importance of vigilance, collaboration and investment in prevention and disruption. The findings present a mixed picture. Some categories recorded fewer incidents or lower losses, while Digital Banking Crime, Card, Vehicle Asset Finance Fraud and Associated Robberies increased. Criminals continued to exploit customer trust, digital channels, financial products, cards and physical cash environments. The figures reflect information reported to SABRIC by participating institutions and should be read together with the data coverage and interpretation notes in each section.

Digital Banking Crime remained one of the most significant reported financial crime risks in 2025. Reported client claim amounts more than doubled from **R1.09 billion** in 2023 to **R2.4 billion** in 2025, representing a **29.2%** increase from approximately **R1.9 billion** in 2024.

Banking App accounted for approximately **89%** of reported Digital Banking Crime cases and **70.5%** of the total client claim amount in 2025. Internet Banking accounted for fewer than **9%** of cases but **28.6%** of the claim amount, showing that a smaller number of cases can still result in substantial financial exposure. Mobile Banking represented fewer than **3%** of cases and less than **1%** of the claim amount but remained relevant because of its association with SIM swap related risk.

Digital Banking Crime was driven mainly by social-engineering and customer compromise and/or manipulation rather than direct attacks on banking systems. Criminals use impersonation, vishing, remote access software, false payment instructions and other forms of manipulation to persuade customers or employees to disclose information, approve access or authorise transactions. Artificial intelligence can make these scams more convincing by helping criminals create realistic messages, images, voices and video content.

Application Fraud showed different trends across the three reported product groups. Vehicle Asset Finance fraud increased materially, with reported fraudulent applications rising by **41%** in 2025. The value of fraudulent applications detected and declined increased by **43.8%** compare to 2024.

Fraudulent Home/Mortgage Loan applications increased slightly by **3.4%**. Potential losses declined by **12.3%**, while reported approved exposure remained broadly stable.

Unsecured Lending Fraud recorded a substantial reduction during 2025. Reported fraudulent applications involving current accounts, savings accounts, credit cards and personal loans decreased by **34%**. Despite this improvement, mule accounts, synthetic identities, first party misrepresentation and AI assisted document manipulation remained important risks.

Card fraud continued to have a substantial financial impact. Gross fraud losses on South African issued credit and debit cards increased by **18%** in 2025. Card Not Present fraud remained the largest identified contributor to losses, although Card Not Present losses declined for both credit and debit cards. Lost and/or Stolen card fraud remained particularly prominent within debit card losses, reinforcing the importance of protecting cards and PINs and reporting missing cards immediately.

Contact crime remained an important operational and security concern in 2025. Incidents declined across most categories, including ATM attacks, bank branch burglaries and bank branch robberies, while associated robberies increased. Although related cash losses decreased, robberies following ATM withdrawals and the use of distraction methods remained important customer safety concerns.

Despite the increase in associated robbery incidents, the related reported cash losses decreased. This shows that the number of incidents and their financial impact did not move in the same direction. The continued prevalence of robberies following ATM withdrawals and the use of distraction methods nevertheless remain important customer safety concerns.

Banking services, whether used digitally or at branches, ATMs and other physical locations, can be used safely when customers remain alert. Criminals often rely on urgency, fear, distraction and misplaced trust. Customers should pause before acting, independently verify unusual requests through official channels, protect their PINs, passwords and one-time passwords (OTPs), remain aware of their surroundings when withdrawing or carrying cash, report lost cards or suspicious transactions to their bank immediately, and report criminal incidents to the South African Police Service (SAPS).

MEMBERS

PARTNERS

DIGITAL BANKING CRIME

Qualification of information

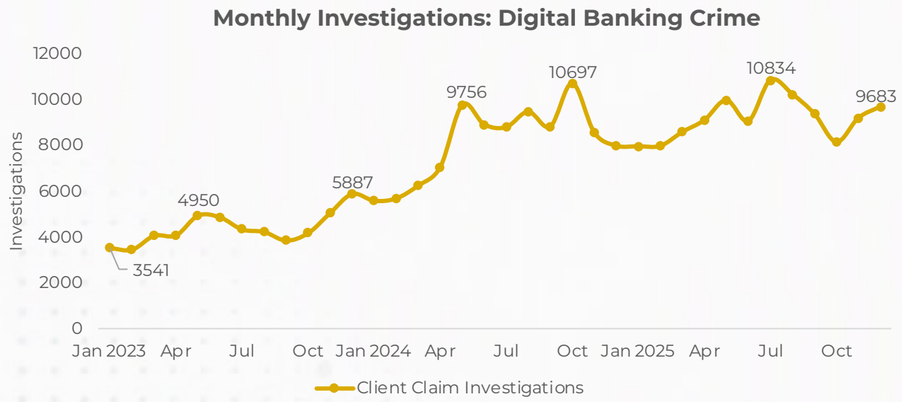
This section is based on Digital Banking Crime data submitted by ABSA, First National Bank, Nedbank, Standard Bank, Capitec Bank, Bidvest Bank, Discovery Bank, Investec and GoTyme Bank. It covers Banking App, Internet Banking and Mobile Banking activity from 1 January 2023 to 31 December 2025. The figures represent client claim amounts and client claim investigations reported by participating SABRIC Members and should not be interpreted as a complete measure of Digital Banking Crime across every bank or financial institution in South Africa.

DIGITAL BANKING CRIME

Digital Banking Crime remained one of the most significant reported financial crime risks in 2025. Reported client claim amounts more than doubled from **R1.09 billion** in 2023 to **R2.41 billion** in 2025, with the 2025 amount representing a **29.2%** increase from approximately **R1.86 billion** in 2024.

Digital Banking Fraud in South Africa

Year	Incidents	Gross Losses	Average Loss per Incident
2023	52 588	R1 085 896 934	R20 649
2024	97 547	R1 862 633 862	R19 095
2025	110 074	R2 406 728 972	R21 865

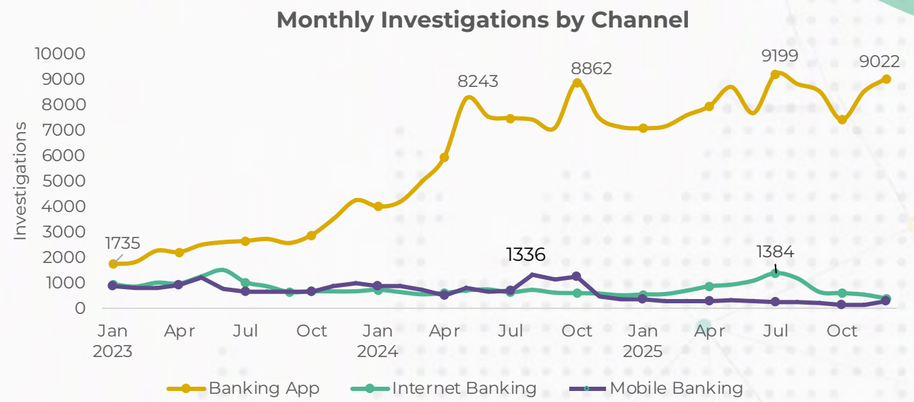


DIGITAL BANKING CHANNELS

Banking App accounted for approximately **89%** of reported cases and about **70.5%** of the total claim amount. Internet Banking accounted for fewer than **9%** of cases but approximately **28.6%** of claim value, showing that a smaller number of cases can still result in substantial financial exposure. Mobile Banking represented fewer than **3%** of cases and less than **1%** of claim value but remained important because of its association with SIM swap-related risk.

Digital Banking Crime by Access Channel during 2025

Crime channel	Total client claims amount	Average monthly claims amount	Share of claims amount	Client-claim investigations
Banking App	R1 696 418 377	R141 368 198	**70.5%**	97 555
Internet Banking	R688 287 956	R57 358 163	**28.6%**	9 354
Mobile Banking	R22 022 639	R1 835 219	**0.9%**	3 165



Banking App

Banking App was the primary channel for Digital Banking Crime in 2025. This does not mean that banking applications or bank systems were compromised. In many cases, the fraud began outside the banking platform, when criminals impersonated trusted organisations, created urgency, or guided customers through transactions in real time. The banking application is used to add beneficiaries, approve payments or move funds after the customer had been deceived.

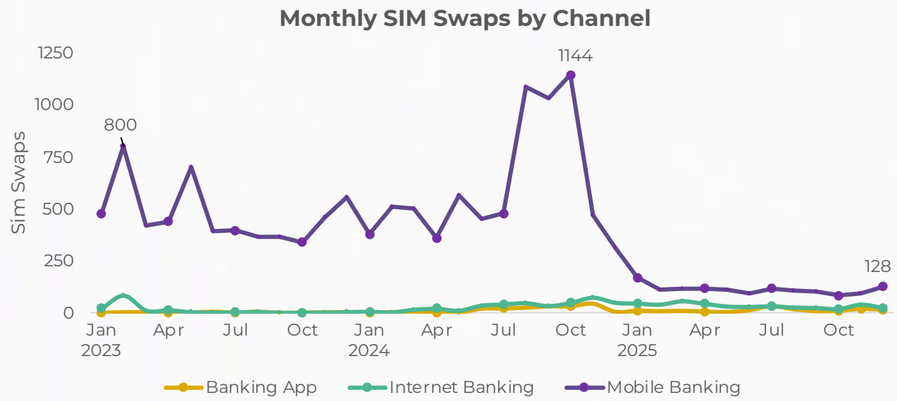
Internet Banking

Internet Banking generated far fewer reported cases than Banking App but accounted for a disproportionately high share of the total claim amount. This channel is often used for larger once-off payments, supplier payments, and business transactions.

Fraudulent beneficiary changes, false payment instructions, and compromised business communications can therefore result in high value losses. Unusual payment instructions received by email, WhatsApp or telephone should be independently verified through a trusted channel before funds are transferred.

Mobile Banking

Mobile Banking contributed a comparatively small share of the total claim amount, but remained relevant because it recorded the highest number of SIM Swap related indicators. Criminals may use a compromised cellphone number to intercept alerts or verification messages and attempt to access banking services.



SIM Swap-linked risks remain relevant because cellphone numbers are often connected to banking alerts, authentication steps, OTPs and customer communication. An unexpected loss of mobile signal, missing verification messages or an unrequested SIM Swap notification should be treated as urgent and reported immediately to both the bank and the mobile network.

COMMON FRAUD SCHEMES AND MODUS OPERANDI DURING 2025

Digital Banking Crime in 2025 was driven primarily by social-engineering-led fraud rather than direct compromise of banking systems. Criminals exploited trust, urgency and real-time interaction with digital channels to persuade customers or employees to disclose information, approve access or authorise transactions. Fraud events often involved multiple overlapping typologies, allowing incidents to progress rapidly from initial contact to financial loss.

Although Banking App activity accounted for most reported Digital Banking Crime incidents, this does not necessarily indicate compromise of banking applications or banking infrastructure. The banking application served as the final transaction channel through which socially engineered or deception-led fraud was executed.

Use of Artificial Intelligence

Artificial intelligence is making some scams more convincing by helping criminals create polished messages, realistic images and believable voice recordings. Industry observations indicate increasing use of AI-generated phishing emails, messaging content and impersonation techniques designed to mimic trusted institutions or individuals. Isolated cases involving cloned voices have also been reported, potentially enabling criminals to impersonate bank officials, company executives or other trusted parties during telephone or video engagements. Although AI remains an enabling rather than primary fraud vector, its use may increase the effectiveness of impersonation, phishing and social-engineering attacks by improving the realism and credibility of fraudulent engagements.

Remote Access and Screen Sharing

Victims were persuaded to install remote-access software or enable screen-sharing functionality under the pretence of receiving technical support, fraud prevention assistance, or account verification services. Once access was granted, criminals could view sensitive information, influence the transaction process, capture credentials, or facilitate transfers to newly added beneficiaries.

Remote-access fraud continued to feature prominently during 2025. Once device control was obtained, funds were typically transferred through a single decisive transaction to a newly created beneficiary, often immediately after access was granted. These incidents frequently progressed rapidly and left limited opportunity for intervention after control of the device had been established.

Impersonation and Vishing

Criminals frequently impersonated banks, law enforcement officials, service providers or other trusted institutions through telephone calls, SMS messages, email and messaging platforms. Victims may be informed that an account is at risk, that a suspicious transaction has occurred, or that funds must be transferred to a so-called safe account. Criminals often remain in contact with victims throughout the process, providing step-by-step instructions and creating urgency that reduces opportunities for independent verification.

Vishing-led authorised payment fraud remained a dominant typology during 2025. Criminals impersonated trusted institutions or officials and coached victims during live telephone engagements to initiate payments through digital banking channels. Transactions were often executed in rapid succession, sometimes to multiple newly created beneficiaries, leaving limited opportunity for interruption once the deception had taken hold. AI-generated messages and voice-cloning capabilities may further increase the credibility of these engagements.

In some incidents, vishing engagements were used to facilitate subsequent remote-access activity, allowing criminals to influence or observe the transaction process directly.

Mule Accounts and the Rapid Movement of Funds

Once funds have been extracted, they were often quickly transferred across multiple accounts, making them more difficult to trace or recover. Mule-enabled fund movement continued to play a significant role, with networks of intermediary accounts facilitating onward transfers, cash withdrawals and rapid balance depletion.

Mule accounts may be controlled by individuals knowingly assisting criminal activity or by persons recruited under false pretences who do not fully understand how their accounts will be used. The rapid movement of funds through multiple accounts reduces opportunities for intervention and recovery.

Industry observations indicated increasing use of digital-asset platforms during fund dissipation phases, enabling criminal proceeds to move rapidly beyond traditional banking channels. Identity compromise, credential theft, synthetic identities, and SIM-swap activity may also be used in combination to facilitate fraud and support the movement and concealment of criminal proceeds.

Marketplace and Supplier Payment Scams

Consumer-focused marketplace scams typically involved transactions that appeared legitimate, including the purchase or sale of goods, vehicle parts or services. Victims were induced to make payments for goods that were never delivered or to release goods based on falsified proof of payment.

In business environments, supplier mandate fraud and business email compromise remained material risks. Criminals redirected payments through fraudulent changes to banking details, falsified supplier information, or compromised communications. These schemes exploited routine business processes, time pressure and trust in established suppliers or counter parties. Funds received through these interactions were frequently withdrawn or transferred shortly after receipt.

Techniques Used to Support Fraud

Across the main fraud methods, criminals repeatedly used the same supporting techniques. These included the misuse of stolen identities, the theft of login details, the use of synthetic identities and the movement of funds through mule accounts. These techniques were often combined, allowing the fraud to progress quickly from initial access or deception to the movement of funds. Although SIM swap activity was less common than in earlier years, it remained relevant in some incidents where criminals attempted to intercept security codes or gain access to accounts. This highlights the importance of monitoring the methods that enable fraud, as well as the main fraud schemes themselves.

International Perspective

International evidence shows a continued shift towards fraud in which criminals manipulate customers or employees into making or approving payments, rather than relying solely on direct attacks against banking systems. The European Banking Authority and European Central Bank[1] reported that manipulation of the payer accounted for more than half of the value of fraudulent credit transfers in the European Economic Area during 2024, while payment users bore approximately **85%** of these losses.

In the United Kingdom, losses arising from authorised push payment fraud increased by **19%** to **£576.4 million** during 2025, while the value of this fraud conducted through mobile banking increased by **28%**. International reporting also highlights increasing criminal use of artificial intelligence to create more convincing phishing campaigns, impersonation attempts and social-engineering engagements.

These international developments remain consistent with observed South African trends, where social engineering, authorised payment fraud and the rapid movement of funds through digital channels continue to be prominent features of the Digital Banking Crime landscape.

Collectively, these fraud schemes demonstrate that Digital Banking Crime is increasingly characterised by deception-led activity rather than direct technical compromise. The convergence of social engineering, remote engagement, mule-enabled fund movement and emerging technologies continues to shape the operational environment within which Digital Banking Crime occurs.

At the UNODC and INTERPOL Global Fraud Summit[2], held in Vienna in March 2026, governments, law enforcement agencies, financial institutions, technology companies and civil society organisations came together to address the growing global threat of fraud. Discussions highlighted the importance of faster cross-border cooperation, stronger public-private partnerships, enhanced prevention measures, improved victim protection and the rapid disruption of fraud networks. The Summit concluded with the adoption of a Call to Action on Combating Fraud and a Global Public-Private Partnership Framework against Fraud and Scams, reflecting increasing international recognition that effective fraud prevention and disruption require coordinated responses across sectors and jurisdictions.

1 *European Banking Authority and European Central Bank. (2025). 2025 Report on Payment Fraud.*

2 *United Nations Office on Drugs and Crime (UNODC). (n.d.). Global Fraud Summit.*

WHAT THE BANKING INDUSTRY IS DOING

Through SABRIC, participating banks have established the Banking Industry Anti-Scam Centre (BIASC), which originated as an industry proof of concept and has since evolved into an ongoing operational capability. Early operational experience has demonstrated that coordinated case handling, structured escalation processes and faster information sharing can significantly reduce response times and improve the ability to identify, trace and preserve funds before they are dissipated through multiple accounts, cash withdrawals, gaming platforms or crypto-asset channels.

While the capability is not yet operating at the scale, coverage or level of automation required to materially reduce overall industry losses, it has generated valuable operational insights and established a foundation for future capability development.

The banking industry continues to work with payment processors, regulators, crypto-asset service providers, gaming platforms, industry bodies, law enforcement agencies and other participants across the fraud ecosystem to strengthen collaboration, improve fraud disruption capabilities and support the development of a future National Anti-Scam Utility capable of operating at greater scale across the broader fraud-response ecosystem.

WHAT THIS MEANS FOR BANKING CUSTOMERS

Digital banking is part of everyday life, and criminals exploit familiar banking routines when customers are busy, worried or under pressure. Customers should stop and verify any unexpected instruction to secure an account, approve a transaction, add a beneficiary, scan a QR code, install remote access software or move money to a so-called safe account. A bank will not ask a customer to disclose a PIN, password or one time password to another person.

- An unexpected call or message creates urgency or fear and demands immediate action.
- Someone asks for a PIN, password, card information or one time password.
- A customer is told to move money to a safe account or approve a transaction that they did not initiate.
- A person asks the customer to install remote access or screen sharing software.
- A beneficiary change or payment instruction is received through email, WhatsApp or telephone and cannot be independently confirmed.
- There is an unexpected SIM swap notification, missing verification messages or a sudden loss of mobile network signal.

When any of these warning signs appear, the safest response is to end the interaction, use an official contact channel to verify the request and report suspicious activity immediately. Customers who unexpectedly lose mobile signal should contact both their bank and mobile network without delay.

CARD FRAUD

Qualification of Information

The Credit and Debit Card Fraud information utilised in this report was provided by ABSA, First National Bank, Nedbank, Standard Bank, Capitec Bank, Access Bank, African Bank, alBaraka Bank, Bidvest Bank, Discovery Bank, Investec, Post Bank, GoTyme Bank, American Express and Diners Club. The statistics used in the report cover the period from 01 January to 31 December 2025. For the comparative analysis, the above-mentioned period was compared to that of 2024.

The information set used was as follows:

- *All calculations are based on the date that the fraudulent transaction occurred.*
- *All fraud losses mentioned refer to gross fraud losses and do not relate to the net losses suffered by the banking industry.*
- *Exact rand values are presented in the tables. In the narrative, fraud loss amounts are generally rounded to one decimal place in millions, unless otherwise stated. As a result, totals calculated from the rounded amounts may differ slightly from the exact totals shown in the tables.*
- *All figures represent gross fraud losses reported to SABRIC by participating card issuers. They do not reflect recoveries, reimbursements or other adjustments and should not be interpreted as the final net loss suffered by the banking industry.*
- *Figures are calculated based on South African Issued Cards and exclude fraud on Fleet Cards and Foreign Issued Card Fraud.*

CREDIT AND DEBIT CARD FRAUD

Gross fraud losses on South African issued credit and debit cards increased by **18.0%**, from approximately **R1.5 billion** in 2024 to **R1.7 billion** in 2025, representing an increase of **R266.3 million**. Credit card fraud losses recorded the largest proportional increase, rising by **29.3%** from **R571.8 million** to **R739.2 million**. Debit card fraud losses increased by **10.9%**, from **R907.3 million** to **R1.0 billion** and remained the largest component of total card fraud losses. However, credit card fraud accounted for approximately **62.9%** of the overall increase in losses.

Gross Fraud Losses: Credit and Debit Cards (All Fraud Types & Countries)

Product	2024	2025	% Change
Gross Fraud Losses (Combined)	R1 479 082 576	R1 745 352 519	**18.0%**
Credit	R571 805 478	R739 234 011	**29.3%**
Debit	R907 277 098	R1 006 118 508	**10.9%**

Gross fraud losses on South African issued cards arising from transactions within South Africa increased by **43.3%**, from **R598.0 million** in 2024 to **R857.5 million** in 2025. Credit card fraud losses increased by **45.8%** to **R301.4 million**, while debit card fraud losses increased by **42.0%** to **R556.0 million**. Debit cards accounted for **64.8%** of domestic card fraud losses and contributed the larger increase in rand value.

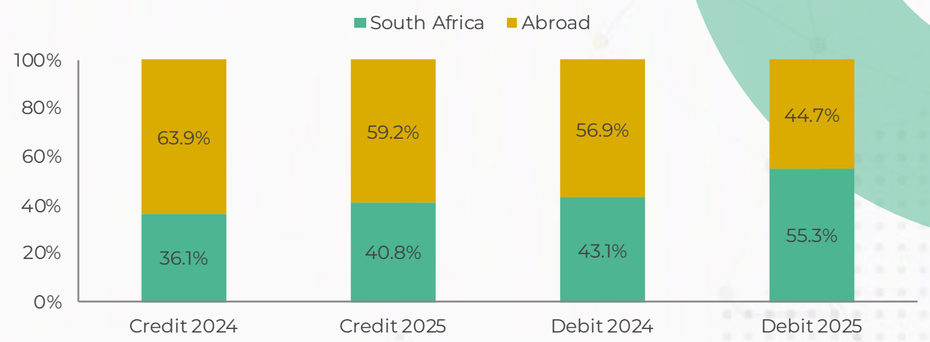
The increase in domestic losses is likely linked to the growing use of cards for online payments, together with a shift towards locally executed Card Not Present and social engineering-related fraud.

Gross Fraud Losses: Credit and Debit Cards (South Africa)

Product	2024	2025	% Change
Gross Fraud Losses (Combined)	R598 056 523	R857 459 174	**43.3%**
Credit	R206 618 822	R301 431 573	**45.8%**
Debit	R391 437 701	R556 027 601	**42.0%**

Within South Africa, card fraud losses were concentrated in Gauteng, the Western Cape and KwaZulu-Natal. Gauteng accounted for **51.7%** of credit card fraud losses and **42.1%** of debit card fraud losses.

Credit and Debit Card Fraud Losses: South Africa vs Abroad: 2024-2025



A significant proportion of fraud involving South African issued cards took place abroad. In 2025, transactions outside South Africa accounted for **59.2%** of credit card fraud losses and **44.7%** of debit card fraud losses. This shows that international transactions continued to represent an important part of the card fraud risk affecting South African issued cards.

The map highlights the leading countries where fraudulent transactions involving South African issued cards were recorded in 2025. The United States ranked highest, while the remaining countries were spread across North America, Europe, and parts of Asia[1].

Gross Fraud Losses: Credit and Debit Cards: Prominent Countries: 2025

1 *The numbered markers indicate ranking only and do not represent transaction volumes, percentages or fraud losses.*

The table below presents the six prominent card fraud types recorded in 2025. Card Not Present fraud was the largest driver of losses for both card types. Lost and/or Stolen card fraud was the second largest fraud type and was particularly prominent within debit card fraud. Together, these two crime types accounted for most of the losses recorded.

Gross Fraud Losses: Credit & Debit Cards: Prominent Fraud Types 2025

Fraud Type[1]	Credit Card	Debit Card	Total
Account Takeover	R 20 997 230	R 7 015 087	**R 28 012 317**
Card Not Present	R 402 109 115	R 378 416 008	**R 780 525 123**
Counterfeit	R 4 362 263	R 13 575 179	**R 17 937 442**
False Application	R 9 012 853	R 14 854 494	**R 23 867 347**
Lost and/or Stolen	R 34 172 551	R 253 002 632	**R 287 175 183**
Not Received Issued	R 708 726	R 1 554 781	**R 2 263 507**

The following section provides further insight in to the prominent card fraud types.

1 *The table includes the six most prominent fraud types only. Other fraud types and losses that could not be classified by fraud type are not included.*

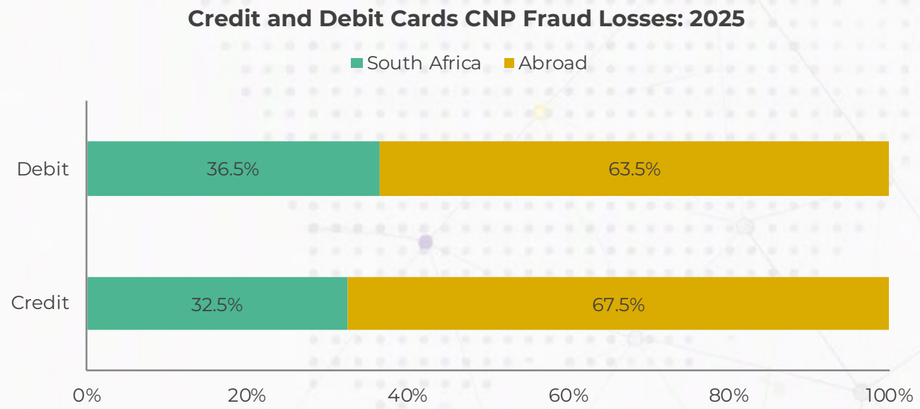
CARD NOT PRESENT (CNP)

Card Not Present fraud losses decreased for both credit and debit cards in 2025. Credit card losses decreased by **5.3%** to **R402.1 million**, while debit card losses decreased by **35.1%** to **R378.4 million**. Despite these reductions, Card Not Present fraud continued to account for a substantial share of overall card fraud losses, representing **54.4%** of credit card losses and **37.6%** of debit card losses.

Gross Fraud Losses: Card Not Present (CNP)

Product	2024	2025	% Change	CNP as % of Gross Fraud Loss
Credit	R424 487 069	R402 109 115	**-5.3%**	54.4%
Debit	R583 478 115	R378 416 008	**-35.1%**	37.6%

Most Card Not Present fraud losses were linked to transactions outside South Africa using South African issued cards. International transactions accounted for **67.5%** of credit card losses and **63.5%** of debit card losses. For credit cards, Advertising services, Travel agencies and Betting accounted for more than half of reported losses. For debit cards, Digital goods, Advertising services and Computer software accounted for **43%**.



Card Not Present fraud is commonly carried out using card information obtained through phishing, vishing and other social-engineering methods. Criminals may impersonate bank officials through calls or messages and deceive customers into disclosing card details and one time passwords (OTP). These details are then used to make unauthorised online transactions, often across borders and through merchant categories where funds can be spent or moved quickly.

International Perspective

Internationally, Card Not Present fraud shows patterns similar to those seen in South Africa. The Australian Payment Fraud Report 2025 found that fraud involving Australian issued cards used at overseas merchants exceeded domestic Card Not Present fraud, highlighting the increased risk associated with international online transactions where authentication controls may differ between countries. It is important to note that the 2025 report presents Australian fraud data for 2024[1].

Broader international payment fraud reporting also shows a growing reliance on social-engineering and customer manipulation. Criminals use methods such as business email compromise and impersonation to deceive customers or employees into sharing information or making payments. This reflects a wider shift towards exploiting trust and authentication processes rather than directly attacking banking systems[2].

1 *Australian Payment Network. (2025). Australian Payment Fraud 2025. January – December 2024 Data*

2 *Nacha. (2022). A New Risk Management Framework for the Era of Credit-Push Fraud*

LOST AND/OR STOLEN CARD FRAUD (L&S)

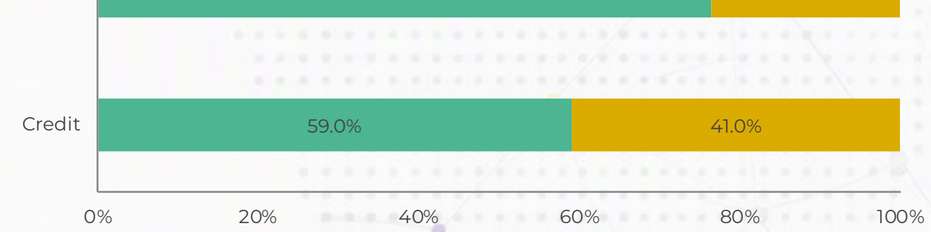
Lost and/or Stolen card fraud showed different trends across the two card products in 2025. Credit card losses decreased by **15.6%** to **R34.2 million** in 2025, while debit card losses remained broadly stable at **R253.0 million**. This fraud type accounted for a much larger share of debit card fraud losses than credit card fraud losses.

Gross Fraud Losses: Lost and/or Stolen Card Fraud (L&S)

Product	2024	2025	% Change	L&S as % of Gross Fraud Loss
Credit	R40 511 605	R34 172 551	**15.6%**	4.6%
Debit	R252 633 375	R253 002 632	**0.1%**	25.1%

Most Lost and/or Stolen card fraud losses occurred within South Africa. For credit cards, Supermarkets, ATMs and Tollgates were among the main merchant groups, with Supermarkets and ATMs together accounting for **40%** of losses. For debit cards, ATMs, Supermarkets and Tollgates were prominent, while ATM withdrawals alone accounted for **49.3%** of losses.

Credit and Debit Cards Lost and/or Stolen Fraud Losses: 2025



Lost and/or Stolen card fraud often involves the physical theft of a card at an ATM through card swapping, distraction or similar methods. Fraudsters may obtain the customer's PIN through shoulder surfing or distraction techniques and then use the card shortly after for cash withdrawals or purchases before it is reported and blocked.

International Perspective

Internationally, Lost and/or Stolen card fraud is less prominent than Card Not Present fraud, but continues to occur in physical payment settings such as retail points of sale and ATMs. The European Banking Authority and European Central Bank reported that fraud involving Lost and/or Stolen or stolen physical cards remains a risk in these channels[1]. Visa has also identified ongoing risks linked to physical card theft and ATM fraud. These trends are consistent with the South African experience, where Lost and/or Stolen card fraud is closely associated with ATM activity and the rapid use of cards before they are reported and blocked[2].

1 *Eba. (2025). European Banking Authority. 2025 Report on Payment Fraud*

2 *Visa Payment Fraud Disruption. (2025). Biannual Threats Report*

ACCOUNT TAKEOVER FRAUD (ACC T/O)

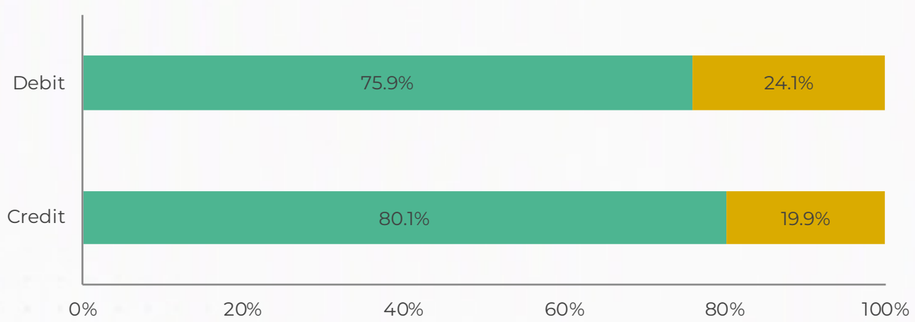
Account Takeover fraud losses increased across both credit and debit cards in 2025. Credit card losses increased by **66.7%**, from approximately **R12.6 million** to **R21.0 million**, while debit card losses increased from approximately **R1.7 million** to **R7.0 million**.

Gross Fraud Losses: Account Takeover Fraud (ACC T/O)

Product	2024	2025	% Change	ACC T/O as % of Gross Fraud Loss
Credit	R12 595 564	R20 997 230	**66.7%**	2.8%
Debit	R1 654 934	R7 015 087	**>100%**	0.7%

Most Account Takeover fraud losses were linked to transactions within South Africa. For credit cards, ATMs, Wholesale Retailers and Supermarkets were among the main merchant groups, with ATM withdrawals accounting for **27.3%** of losses. For debit cards, Wholesale Clubs (accounting for **33.9%** fraud losses), Foreign Currency Agencies and Supermarkets were prominent.

Credit and Debit Card Acc T/O Fraud Losses: 2025



Account Takeover fraud usually begins when fraudsters obtain a customer's banking or card credentials through phishing emails, malicious links or phone calls in which they impersonate bank officials. Customers may be persuaded to disclose login details or one-time passwords (OTP), allowing criminals to access the account, conduct unauthorised transactions and move or withdraw funds through ATMs and retail transactions.

International Perspective

International reporting shows that Account Takeover fraud is increasingly driven by phishing, impersonation and other social-engineering methods used to obtain customer credentials or manipulate authentication processes[1]. Criminals may persuade customers to disclose login information, approve access to their accounts or authorise payments under false pretences, often through impersonation or business email compromise schemes[2]. These trends are consistent with the South African experience, where Account Takeover fraud is closely linked to compromised credentials and the exploitation of customer trust rather than direct attacks on banking systems.

1 *European Payments Council. (2025) 2025 Payment Threats and Fraud Trends Report*

2 *Nacha. (2022). A New Risk Management Framework for the Era of Credit-Push Fraud*

FALSE APPLICATION FRAUD (F/APP)

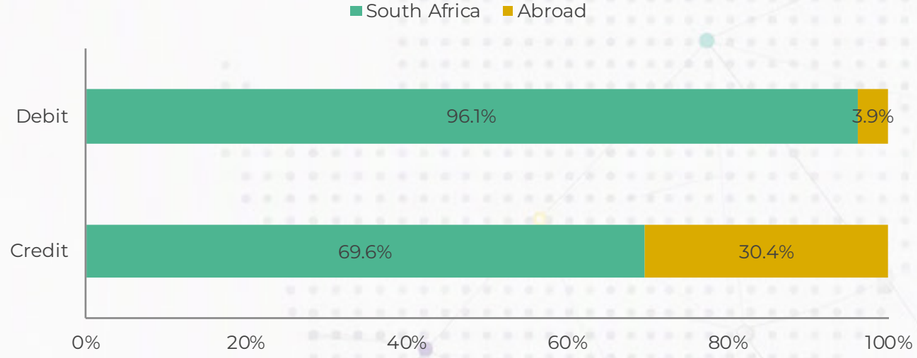
False Application Fraud losses moved in opposing directions across the two card products in 2025. Credit card losses decreased by **45.8%**, from **R16.6 million** to **R9.0 million**, while debit card losses increased by **88.7%**, from approximately **R7.9 million** to **R14.9 million**. Combined losses decreased slightly by **2.6%** to **R23.9 million**.

Gross Fraud Losses: False Application Fraud (F/App)

Product	2024	2025	% Change	F/App as % of Gross Fraud Loss
Credit	R16 638 652	R9 012 853	**-45.8%**	1.2%
Debit	R7 871 401	R14 854 494	**88.7%**	1.5%

Most losses were linked to transactions within South Africa. For credit cards, ATMs, Manual Cash Disbursements and Supermarkets were among the main categories. Debit card losses were largely concentrated at ATMs, with withdrawals accounting for **78.9%** of losses.

Credit and Debit Cards F/App Fraud Losses: 2025



False Application Fraud involves the use of stolen, fabricated or synthetic identities to open accounts or obtain card facilities. Once an application is approved, criminals use the account or card shortly after to withdraw cash or move funds before the fraud is detected.

International Perspective

Internationally, False Application Fraud is closely linked to identity misuse, synthetic identities and fraudulent account opening. Experian reports that advances in generative artificial intelligence are enabling criminals to create increasingly realistic false identities, making detection more difficult[1].

The European Payments Council also identifies onboarding and authentication processes as areas that criminals target when attempting to obtain accounts or payment facilities. These patterns are consistent with the South African experience, where stolen, fabricated or synthetic identities are used to obtain accounts or card facilities that are exploited soon after approval[2].

1 *Experian. (2026). The new identity challenge: How AI is transforming fraud and digital trust.*

2 *European Council. (2025). 2025 Payment Threats and Fraud Trends Report*

APPLICATION FRAUD

Qualification of information

The fraud-related information used in this report was provided by ABSA, First National Bank, Nedbank, Standard Bank, Capitec Bank, Access Bank, Bidvest Bank and GoTyme Bank. The statistics cover the period from 1 January to 31 December 2025 and are compared with the equivalent 2024 period. All figures and calculations are based on Application Fraud data reported to SABRIC.

Figures reflect only fraud cases reported to SABRIC and exclude cases that remain under investigation. As fraud investigations can take an extended period to conclude, losses associated with these cases are not reflected in the reported figures.

Definitions used in this report

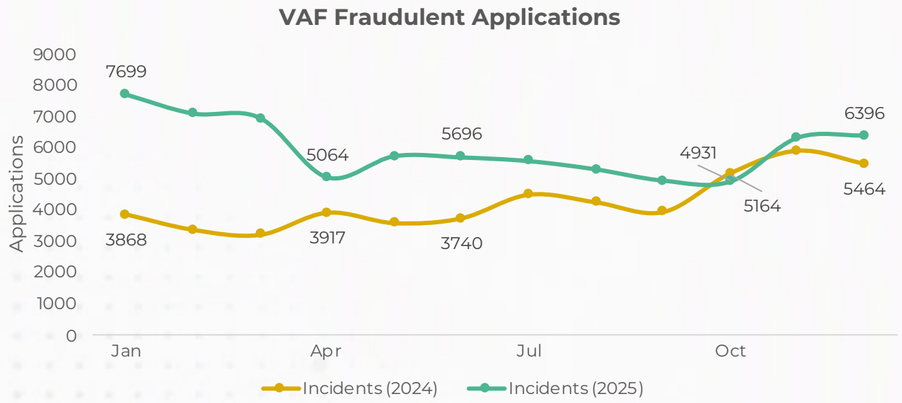
- *Reported applications/incidents: the number of fraudulent applications reported for the product during the period.*
- *Potential loss: the value of fraudulent applications that were detected and declined before approval.*
- *Actual loss: the value of fraudulent applications that were approved and therefore became realised or approved exposure.*
- *Total fraud exposure: potential declined loss plus approved/actual loss.*
- *The report distinguishes between the number of fraudulent applications reported, the value of fraudulent applications prevented before approval, and the value of fraudulent applications that were approved and resulted in actual financial exposure. Where the prevented and actual amounts are combined, the total is described as total fraud exposure. This distinction is important because not all attempted fraud has resulted in a financial loss.*

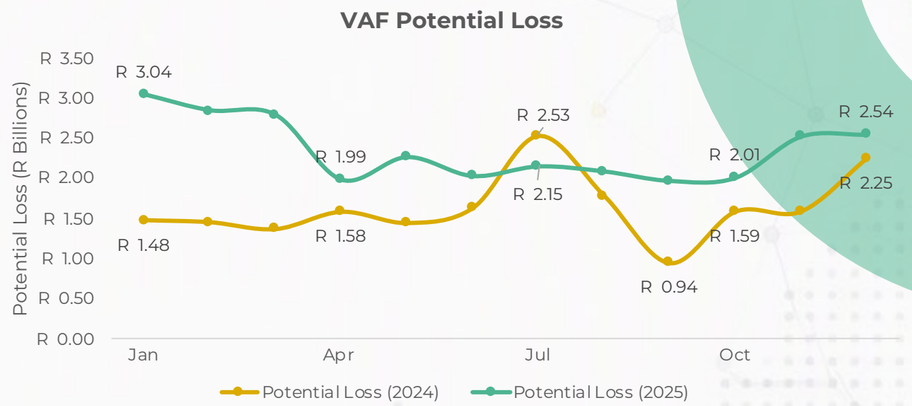
VEHICLE ASSET FINANCE FRAUD

Vehicle Asset Finance fraud in South Africa continues to be driven by a small number of established criminal methods. Although syndicates have refined how these schemes are carried out through greater coordination and the use of supporting technologies, the main risks remained consistent in 2025. These included vehicle identity manipulation, unlawful changes to ownership records, and fraudulent applications based on false or manipulated identities and applicant profiles.

Vehicle Asset Finance Fraud (VAF)

Measure	2024	2025	% Change
Reported applications/incidents	50 885	71 747	**41.0%**
Potential loss	R19.7bn	R28.3bn	**43.8%**





Note: Actual losses have been excluded from the year-on-year comparison as 2025 information remains incomplete at the reporting cut-off date. Some cases are still under investigation, and the related financial information has not yet been submitted to SABRIC.

Cloned Motor Vehicles

Cloned vehicles remain a persistent and damaging form of Vehicle Asset Finance fraud. Stolen or hijacked vehicles are given the identity of legitimate vehicles through changes to vehicle-identification number (VIN) plates, chassis markings and registration records. Rapid ownership transfers may then be used to conceal the vehicle's history before it is sold to an unsuspecting buyer or financed through a legitimate institution.

A significant development in 2025 was the Special Investigating Unit's work on transport and licensing irregularities, including the manipulation of eNaTIS records. This resulted in the recovery of **R14.7 million** in irregularly diverted funds and the cancellation of more than **190 000** fraudulent licences, highlighting weaknesses in the registration environment that may allow cloned vehicles to circulate before they are detected.[1] Financial institutions have strengthened controls through physical vehicle inspections and data verification, although weaknesses in the broader registration system remain a challenge.

1 *IOL. (2025). R14.7m reclaimed in eNaTIS fraud probe. Independent Online, 4 December 2025.*

Illegal Change of Vehicle Ownership or Title

Illegal changes to vehicle ownership or title remain a serious form of Vehicle Asset Finance fraud and are often linked to vehicle cloning. Criminals may unlawfully remove the lender as the registered titleholder, allowing the vehicle to be registered in another name, sold locally or moved across the border before the fraud is detected. This significantly reduces the likelihood of recovery, particularly once the vehicle has left South Africa. During 2025, South African Police Service operations disrupted parts of organised vehicle smuggling networks operating between KwaZulu-Natal and Mozambique, resulting in arrests and the recovery of stolen vehicles, some of which were linked to false registration documents. In many cases, vehicles are moved shortly after finance is granted and before missed payments alert the lender to possible fraud.[1]

International Perspective

Internationally, Vehicle Asset Finance fraud follows patterns similar to those seen in South Africa, with identity misuse, false income or employment information, first party fraud and the rapid movement or disposal of financed vehicles remaining key concerns. Point Predictive's 2026 Auto Lending Fraud Trends Report, which examined United States data for 2025, estimated fraud exposure at **US$10.4 billion**, approximately **13%** higher than the previous year. First party fraud accounted for around **69%** of this exposure, while income and employment misrepresentation and the growing use of AI generated supporting documents continued to increase the sophistication of fraudulent applications. [2]

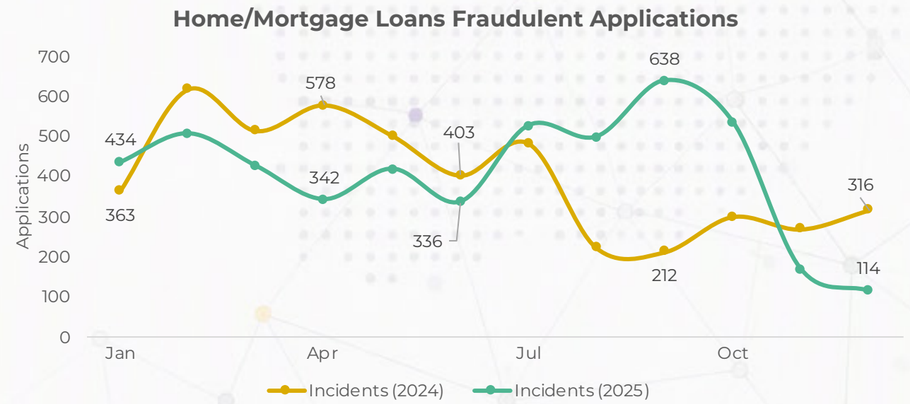
HOME/MORTGAGE LOAN FRAUD

Reported fraudulent Home/Mortgage loan applications increased slightly by **3.4%**, between 2024 and 2025. The value of fraudulent applications identified before approval decreased by **12.3%** in the same period, while actual losses remained broadly stable.

Home/Mortgage Loan Fraud

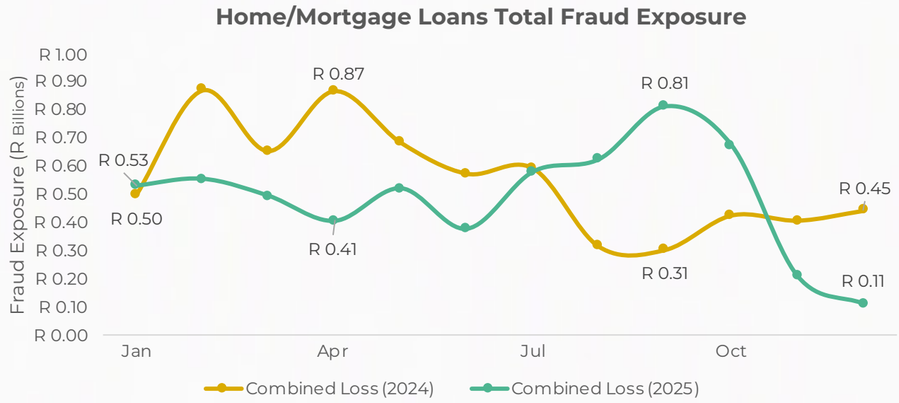
Measure	2024	2025	% Change
Reported applications/incidents	4 780	4 942	**3.4%**
Potential loss	R6.1bn	R5.3bn	**-12.3%**
Actual loss	R599.7m	R595.9m	**-0.6%**

Where the province in which the application originated could be determined, Gauteng accounted for **60%** of reported applications, followed by the Western Cape at **20%** and KwaZulu-Natal at **10%**. Although the underlying property may provide some security for the loan, banks can still incur significant legal, recovery and eviction costs when fraudulent applications are approved.



1 *IOL. (2025). How SAPS cracked a vehicle-smuggling chain moving cars from KwaZulu-Natal to Mozambique. Independent Online, 14 December 2025.*

2 *Point Predictive. (2026). 2026 Auto Lending Fraud Trends Report: Fraud exposure reaches record USD 10.4 billion.*



Home/Mortgage loan fraud in South Africa is driven mainly by false or misleading information provided during the loan application process. Applicants may submit altered, incomplete or fabricated information to improve their chances of approval, obtain a larger loan than they qualify for, or create the appearance that they can afford the repayments. The most common methods include false income and employment information, manipulated credit profiles, synthetic identities, fraudulent supporting documents and coordinated syndicate activity.

Income and Employment Misrepresentation

The most common form of Home/Mortgage loan fraud involves applicants providing false or inflated information about their income or employment. This may include falsified payslips, employment letters and bank statements designed to create the impression that the applicant earns more, has more stable employment or can afford a larger loan than is supported by their actual financial position.

A 2025 South African consumer survey found that **26%** of respondents believed it was sometimes acceptable to overstate income when applying for credit, highlighting the need for stronger income and employment verification and greater public awareness of the consequences of providing false information.

International Perspective

International reporting shows that mortgage fraud remained centred on false income and employment information, identity manipulation and deception during the application process. Cotality reported that approximately one in every **118** mortgage applications displayed potential fraud indicators by the end of 2025, with investment properties and multi-unit residential buildings identified as higher risk categories. As in South Africa, synthetic identities and the growing use of artificial intelligence to create false documents or manipulate identity verification processes are becoming increasingly important fraud risks.[1, 2]

1 FICO. (2025). FICO survey shows South Africans will bend the truth to access credit.

2 Cotality. (2025). Mortgage fraud risk continues its upward trend to end 2025.

UNSECURED LENDING FRAUD

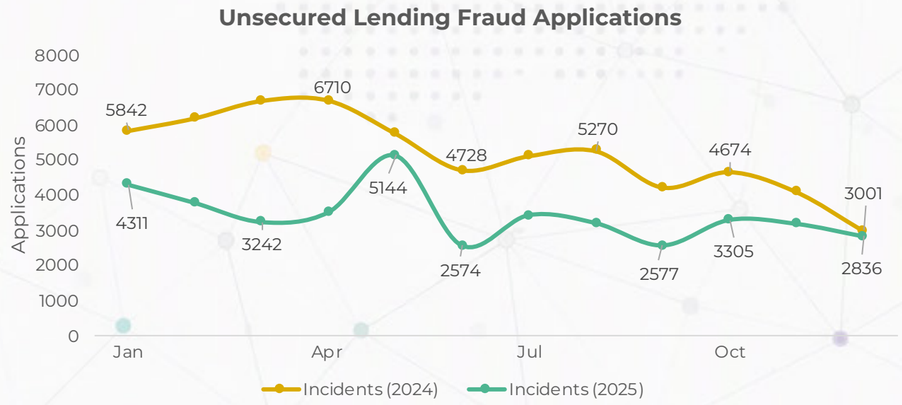
Unsecured Lending Fraud involves fraudulent applications for products that do not require collateral, including current and savings accounts, credit cards and personal loans. Reported fraudulent applications decreased by **34%** between 2024 and 2025.

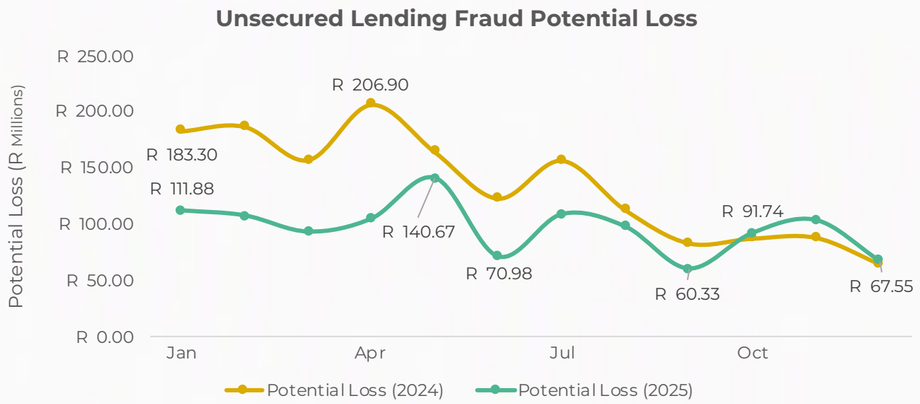
Unsecured Lending Fraud

Measure	2024	2025	% Change
Reported applications/incidents	62 367	41 148	**-34.0%**
Potential loss	R1.6bn	R1.2bn	**-28.5%**

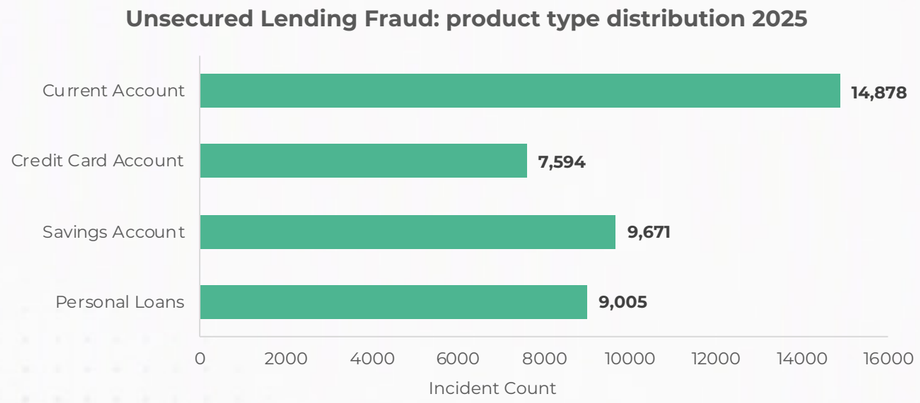
The value of attempted fraudulent applications decreased by **28.5%** in the same period. Where the province in which the application originated could be determined, Gauteng accounted for **68%** of reported applications, followed by KwaZulu-Natal and the Western Cape at **9%** each.

Current account applications represented the largest share of reported Unsecured Lending Fraud in 2025, accounting for **36%** of fraudulent applications. Savings account applications followed at **24%**, while personal loan applications accounted for **22%** and credit card account applications for **18%**. This distribution indicates that Unsecured Lending Fraud was concentrated primarily in account-opening products and other facilities that provide relatively rapid access to banking services, credit or funds, allowing criminals to move or utilise proceeds soon after approval.





Note: Actual losses have been excluded from the year-on-year comparison as 2025 information remains incomplete at the reporting cut-off date. Some cases are still under investigation, and the related financial information has not yet been submitted to SABRIC.



Unsecured Lending Fraud is largely committed during the application process for products such as personal loans, credit cards and bank accounts, where no asset is provided as security. Criminals exploit the speed at which these products can be approved and funds made available, then move the money rapidly through mule accounts or other linked accounts to make tracing and recovery more difficult. The main methods include false or synthetic identities, first party misrepresentation, coordinated syndicate activity and the use of altered or AI generated supporting documents.

Mule Accounts and Fund Funnelling

Mule accounts remain a central feature of Unsecured Lending Fraud. Criminals may apply for bank accounts, credit facilities or personal loans using valid (given voluntarily or stolen) identities, fabricated identities or synthetic identities, and then move the approved funds through one or more mule accounts to conceal the money trail and make recovery more difficult[6].

These accounts may be opened by individuals who knowingly assist criminals or by people who have been recruited without fully understanding how their accounts will be used. Once the funds have been transferred through the network, the original account or loan is often left unpaid, resulting in a loss to the financial institution. This method is particularly effective in unsecured products because funds can be accessed and moved quickly after approval[7].

International Perspective

Internationally, fraud risks linked to unsecured products and account-opening processes continued to evolve during 2025, with reporting highlighting mule networks, synthetic identities, first-party fraud and new-account fraud as persistent concerns[1, 2, 3]. First-party fraud accounted for **36%** of fraud events, while synthetic identity fraud increased eightfold year on year and was increasingly enabled through the use of generative AI to create sophisticated synthetic identities. In the United Kingdom, identity fraud remained the most prevalent case type and false applications continued to increase[4]. In the United States, **503 450** credit card fraud cases were reported during the first three quarters of 2025, with new-account fraud accounting for the majority of reported Credit Card Fraud cases[5].

1 *LexisNexis Risk Solutions. (2026). Global fraud trends and credit-risk fraud reporting.*

2 *Biometric Update. (2026). Synthetic identity fraud soared 8x in 2025.*

3 *Motley Fool Money. (2025). Identity theft and credit-card fraud statistics.*

4 *Cifas. (2026). Fraudscape 2025: Record fraud levels.*

5 *Federal Trade Commission (FTC). (2025). Identity theft and credit-card fraud data.*

6 *TransUnion. (2025). 2025 H2 Top Fraud Trends Report.*

7 *European Payments Council (EPC). (2025). 2025 Payments Threats and Fraud Trends Report.*

GENERAL APPLICATION FRAUD TRENDS

Profile Building and Identity-Based Application Fraud

Vehicle Asset Finance and Home/Mortgage Loan fraud increasingly involve the creation of seemingly legitimate applicant profiles. Criminals may use compromised identity information, shared addresses, falsified employment and income details, and fraudulent supporting documents to strengthen applications and secure high-value vehicles or larger home loans than would otherwise qualify for approval.

In some cases, individuals or syndicates further enhance these profiles by creating the appearance of regular income, stable cash flow and responsible account management through activity that does not reflect genuine earnings. This may enable applicants with limited or poor credit histories to appear eligible for substantial finance and circumvent affordability assessments, credit evaluations and other verification controls.

These methods demonstrate how identity misuse, profile manipulation, income misrepresentation and document fraud continue to play a significant role in Vehicle Asset Finance and Home Loan Application Fraud.

Synthetic Identities, First-Party Fraud and AI-Assisted Fraud

Fraudsters increasingly use synthetic identities, combining genuine and fabricated personal information to create applicant profiles that appear legitimate[1,2]. These profiles may be used to support account-related fraud, credit applications or other fraudulent application activity[1, 2, 3].

First-party fraud occurs when individuals use their own identities but provide false information about their income or financial circumstances. Artificial intelligence further increases the effectiveness of these methods by enabling forged documents, deepfakes and impersonation during digital verification or onboarding processes[1]. Economic pressures and the growing availability of these technologies have increased the complexity of detecting Application Fraud[1, 3].

1 *TransUnion Africa. (2025). AI-powered fraud and deepfake scams.*

2 *Biometric Update. (2026). Synthetic identity fraud soared 8x in 2025.*

3 *FICO. (2025). FICO survey shows South Africans will bend the truth to access credit.*

CONTACT CRIME

Qualification of information

This report summarises contact crime incidents affecting SABRIC member institutions that were reported to SABRIC during 2024 and 2025.

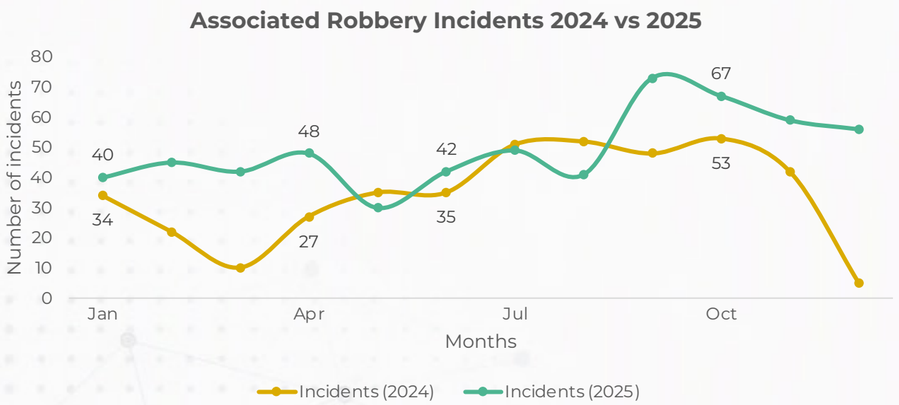
ASSOCIATED ROBBERY

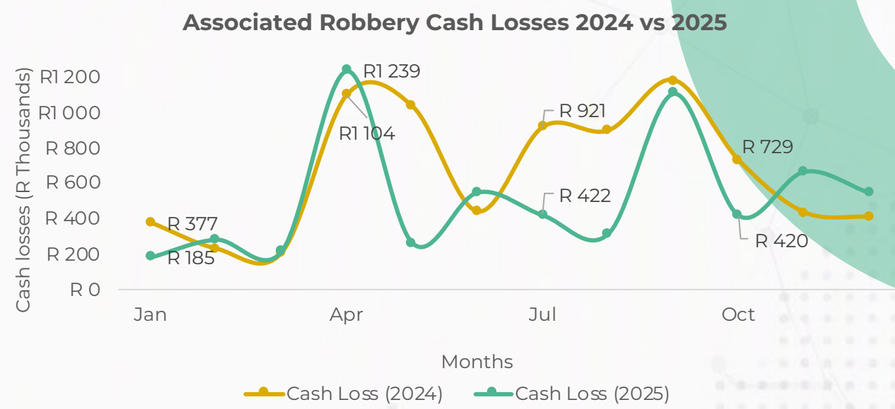
Specific data clarification: Associated Robberies may be recorded by the South African Police Service under broader crime classifications, including common robbery or robbery with aggravating circumstances. In addition, some customers report incidents to their bank without opening a case with the police. The figures therefore represent incidents reported to and known by SABRIC and should not be interpreted as a complete measure of every associated robbery in South Africa.

Associated Robbery Incidents and Cash Losses

Measure	2024	2025	% Change
Incidents	414	592	**43%**
Cash Losses	R7 976 439	R6 236 770	**-22%**

Reported associated robbery incidents increased by **43%**, from **414** in 2024 to **592** in 2025. Despite the increase in incidents, reported cash losses decreased by **22%**.





Incidents and Cash Losses per Sub Type

Incident Sub-Type	Incidents		Cash Loss	
	2024	2025	2024	2025
Associated Robbery - Branch Before Deposit	26	34	R1 956 916	R1 468 975
Associated Robbery - ATM After Withdrawal	154	257	R537 405	R1 096 851
Associated Robbery - ATM before Deposit	78	49	R1 339 895	R544 280
Associated Robbery - Branch After Withdrawal	55	50	R2 941 595	R924 646
Associated Robbery - Inside Branch	1	1	R100 000	R73 110
Associated Robbery - Other - Money bomb	64	132	R358 657	R947 468
Associated Robbery - Other - Muti-related	22	54	R591 471	R969 040
Associated Robbery - Other - Theft out of vehicle	0	1	R0	R8 000
Associated Robbery - Other (Determined by MO)	14	13	R150 500	R174 400
Associated Robbery - Other - Competition Scam	0	1	R0	R30 000
Associated Robbery Total	**414**	**592**	**R7 976 439**	**R6 236 770**

Although the number of reported Associated Robbery incidents increased in 2025, the total reported cash losses decreased. The rise in incidents was driven primarily by robberies following ATM withdrawals, together with significant increases in money bomb incidents and those classified as muti-related. Both money bomb and muti-related incidents more than doubled during 2025.

Customers are particularly vulnerable immediately after withdrawing cash from an ATM. The increase in associated robbery incidents during 2025 was driven mainly by robberies following ATM withdrawals. Incident analysis indicates that **43%** of these incidents occurred during the first eight days of the month, which coincides with SASSA payment periods and month end salary withdrawals. Criminals may observe a customer withdrawing cash, follow the customer and commit the robbery after the customer has moved away from the ATM. The robbery may take place in a parking area,

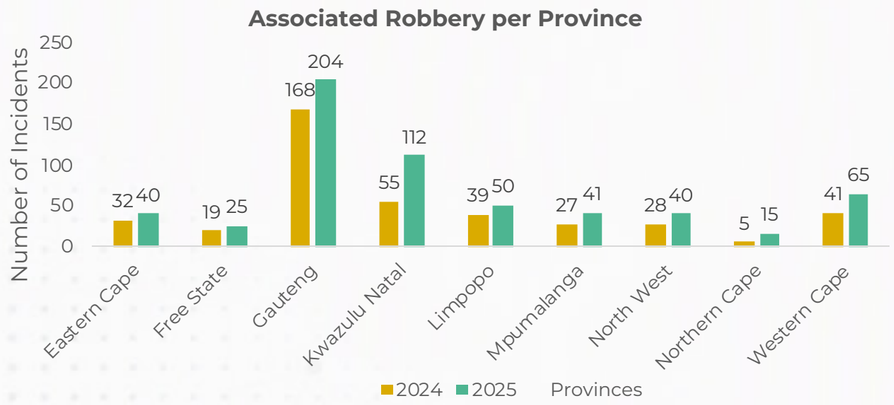
at another business, while the customer is travelling, or after the customer has reached another destination.

In a money bomb incident, criminals place a fake bundle of money where a customer is likely to notice it. Once the customer shows interest, accomplices may approach and claim ownership of the money, suggest that it should be shared, lure the customer to another location, or impersonate police officers investigating the money. The criminals then use the confusion or isolation of the customer to steal the cash that was recently withdrawn.

In incidents classified by SABRIC as muti-related, criminals may place or smear an unknown substance on a customer's clothing or body after the customer has withdrawn cash. They then draw attention to the substance, offer assistance or create confusion. While the customer is distracted, the criminals steal the cash. This description relates to the criminal method recorded in SABRIC's data and should not be interpreted as referring to traditional healing practices generally.

Robberies following withdrawals at bank branches declined during 2025, together with the associated cash losses. This improvement was supported by the arrest of key suspects linked to this crime type, as well as the timely sharing of intelligence and risk information with bank branches, which enabled staff and security teams to identify suspicious behaviour, strengthen preventative measures and respond more effectively.

However, the increase in robberies following ATM withdrawals and in distraction based methods shows that customer safety remains a serious concern. Customers should remain alert after withdrawing cash, avoid displaying or counting cash in public, decline assistance from strangers, avoid accompanying anyone to another location, and immediately contact their bank or the South African Police Service if they notice suspicious behaviour.



Associated robbery incidents increased across all nine provinces in 2025, with Gauteng remaining the main concentration, KwaZulu-Natal recording the largest increase and the Western Cape reporting the highest cash losses after Gauteng, highlighting the need for targeted customer awareness and law enforcement interventions in the most affected provinces while maintaining vigilance nationally.

International Perspective

Although the term associated robbery is used mainly in South Africa, similar crimes occur internationally under names such as bank jugging, follow home robbery, pigeon drop scams and ATM distraction theft.[1] [2] [3]These crimes generally involve selecting a customer at a bank or ATM, observing a cash withdrawal, creating a distraction before following, deceiving, intimidating or luring the customer to another location where the recently withdrawn cash is stolen.[1] [2] [3] While the terminology and methods differ, the common features are the targeting of customers around cash withdrawal points, the use of surveillance or distraction, and the theft of cash after the customer has left the bank or ATM.[1] [3]

1 *The Independent. (2025). "'Bank jugging' thieves strike across California, robbing people after ATM withdrawals." Published 19 July 2025.*

2 *Los Angeles County District Attorney's Office. (2016). "Seniors Get Duped in Pigeon Drop Scam." Published 27 May 2016.*

3 *San Joaquin County District Attorney's Office. (2025). "Avoid the ATM Distraction Scam." Published 26 November 2025.*

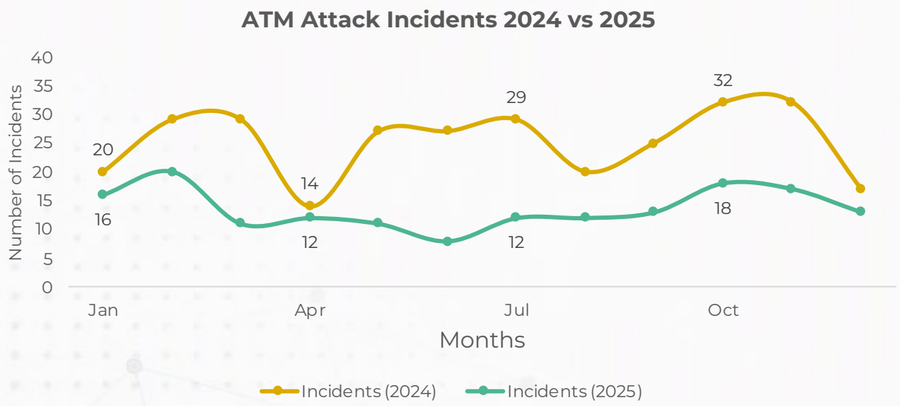
ATM ATTACKS

ATM Attack incidents may be reported to SABRIC by member and non-member institutions, as well as by third parties such as shopping centres, service stations and other site operators. These incidents are attributed to the relevant crime category. While all reported incidents are included in the analysis, the cash loss figures presented below are limited to losses incurred by SABRIC member institutions.

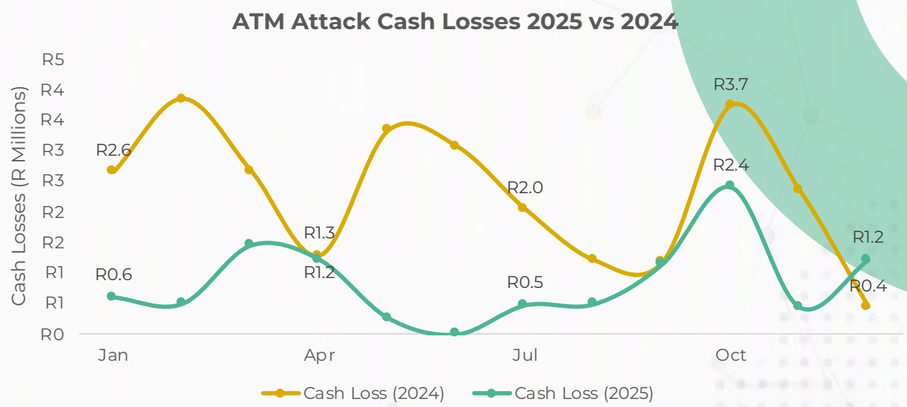
ATM Attack Incidents and Cash Losses

Measure	2024	2025	% Change
Incidents	301	163	**-46%**
Cash Losses	R27 688 690	R10 185 900	**-63%**

Reported ATM attacks decreased by **46%** during 2025, while the associated cash losses declined by **63%**.



ATM attack incidents remained below the corresponding 2024 periods throughout 2025, indicating that the annual decline was sustained across the reporting period rather than being driven by one or two unusually low months. Although incidents increased modestly during the second half of 2025, they remained below the levels recorded during the same period in 2024. The factors contributing to the decline are discussed below where they are supported by confirmed operational information.



Incidents and Cash Losses per Sub Type

Incident Sub-Type	Incidents		Cash Loss	
	2024	2025	2024	2025
ATM Attack - Burglary	21	12	R0	R0
ATM Attack - Cutting Torch	1	4	R0	R0
ATM Attack - Explosives	254	107	R25 349 860	R7 686 870
ATM Attack - Grinder	16	25	R2 092 150	R2 499 030
ATM Attack - Theft	3	7	R0	R0
ATM Attack - Tools	6	8	R246 680	R0
ATM Attack Total	**301**	**163**	**R27 688 690**	**R10 185 900**

ATM attacks involving explosives decreased by **58%** in 2025. Perpetrators accessed the cash in **81%** of these incidents and, although dye staining systems were activated, offenders still removed stained cash in several incidents. Gauteng recorded **31%** of incidents, followed by Mpumalanga at **20%**, with Tshwane and Gert Sibanda the most affected districts. These attacks are often carried out rapidly at service stations and smaller retail locations, particularly where multiple ATMs are situated in close proximity. In some cases, perpetrators also robbed service station convenience stores or targeted drop safes during the attack.

The decline was supported by targeted collaboration between the banking industry and the South African Police Service. Across all ATM attack types, incidents in Gauteng decreased from **201** in 2024 to **61** in 2025, while reported cash losses declined from **R20.7 million** to **R2.6 million**. Project Big Bang contributed to the identification and arrest of nearly **50** suspects linked to this crime type. Stronger site protection, roller shutter doors, protective ATM cages, intelligence sharing, hotspot monitoring and improved response coordination also helped to disrupt repeat attacks, particularly in Soweto, Ekurhuleni and high-risk service station locations.

ATM attacks involving angle grinders increased by **56%**, from **16** incidents in 2024 to **25** in 2025. Perpetrators accessed the cash in **48%** of these incidents, including cases where the cash was dye stained. These attacks generally involve a coordinated group targeting ATMs in shopping centres. Security guards may be held hostage while perpetrators dressed in security uniforms keep watch and others use angle grinders to access the ATM safe. The method requires time, coordination and several perpetrators to execute a successful attack.

ATM theft incidents increased by **133%**, with seven incidents recorded during November and December 2025. These attacks may involve organised criminal groups of up to **20** suspects, who primarily target ATMs located at retail premises. Perpetrators often use grinders to breach roller shutter doors before physically removing the ATM from the premises by various means. The ATM is then transported, often with the aid of a trolley, to a light delivery vehicle and taken to a secondary location, where the safe is forcibly breached and the cash extracted.

Incidents and Cash Losses per Province

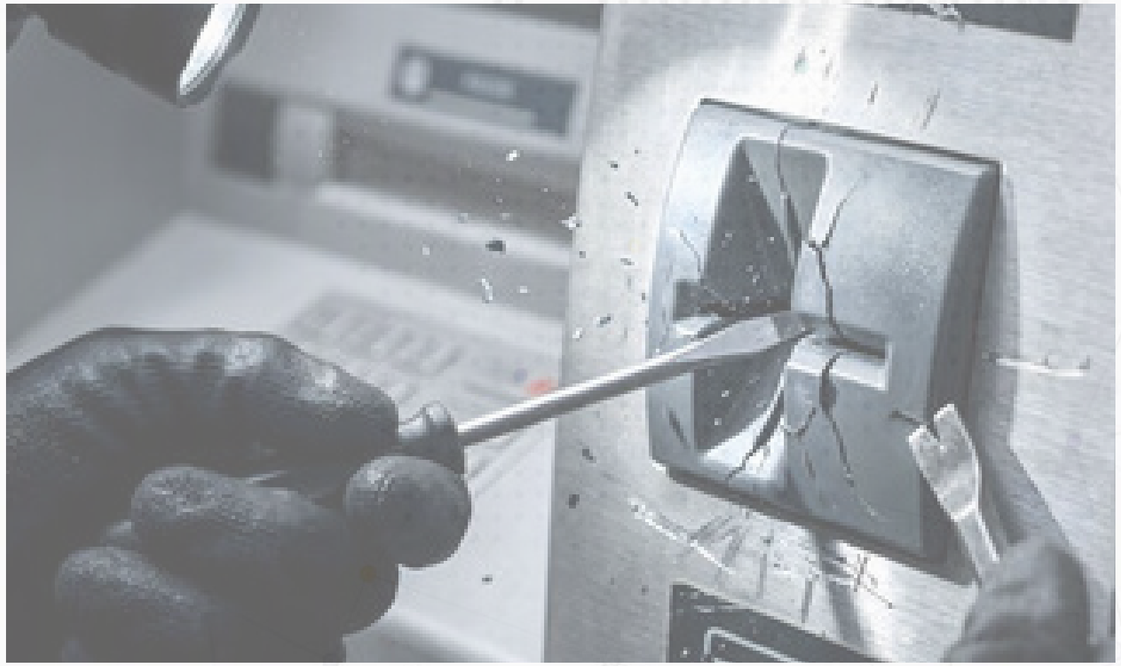
Province	Incidents		Cash Loss	
	2024	2025	2024	2025
Eastern Cape	18	16	R816 370	R1 337 260
Free State	13	14	R1 179 890	R956 700
Gauteng	201	61	R20 706 730	R2 643 830
KwaZulu-Natal	3	2	R0	R527 650
Limpopo	29	17	R2 454 940	R916 000
Mpumalanga	11	25	R1 134 260	R2 281 450
Northwest	21	22	R1 396 500	R1 333 080
Northern Cape	3	4	R0	R0
Western Cape	2	2	R0	R189 930
ATM Attack Total	**301**	**163**	**R27 688 690**	**R10 185 900**

Nationally, ATM attack incidents decreased by **46%** and reported cash losses by **63%** in 2025, with the improvement driven mainly by the sharp reduction recorded in Gauteng following focused interventions. The decline was not uniform across the country, however, as Mpumalanga recorded increases in both incidents and losses, while the Eastern Cape and KwaZulu-Natal experienced higher losses despite relatively low incident volumes. Limpopo improved, the Free State and Northwest remained broadly stable, and the remaining provinces continued to report comparatively low levels of activity. Overall, the provincial pattern indicates that ATM attack risk reduced nationally but shifted geographically, requiring continued monitoring and targeted responses in emerging hotspots.

International Perspective

International evidence shows that ATM attacks are evolving rather than disappearing, although trends differ between regions.[1] [2] [3] The European Association for Secure Transactions reported **5,953** ATM related physical attacks across **19** European countries in 2024, an increase of **28%** from 2023.[1] Within this total, attacks involving explosives decreased by **16%**, while ATM theft and burglary increased by **17%**.[1] Explosives nevertheless accounted for **71%** of reported physical attack losses, and the related damage to ATMs and surrounding buildings was not included in these loss figures.[1]

An industry report published by the American Bankers Association reported that physical attacks accounted for **66%** of ATM crime, while jackpotting attacks increased from **200** incidents in 2023 to more than **300** in 2024.[2] The same report estimated that approximately **US$27,000** was stolen per attack on average, while replacing a damaged ATM could cost more than **US$50,000**.[2] These findings show that the impact of ATM crime extends beyond stolen cash to include equipment replacement, damage to surrounding property and disruption to ATM services.[1] [2] [3] They also support the continued use of layered security measures, including surveillance, physical barriers, rapid response and cash tracking technology.[2] [3]



1 *European Association for Secure Transactions. (2025). European Terminal Fraud Attacks Double. Published 14 April 2025.*

2 *American Bankers Association. (2025). ATM Crime Trends in 2025. Industry information prepared by 3SI and published on 1 July 2025.*

3 *ATM Industry Association. (2024). New Trends in ATM Fraud. Published 19 December 2024.*

BANK BURGLARY

Bank branch burglary incidents decreased by **19%**, from **27** in 2024 to **22** in 2025, while reported cash losses increased by **52%**, from approximately **R1.5 million** to **R2.2 million**. This means that fewer incidents were recorded, but losses were concentrated in a smaller number of higher value, cash focused attacks. In 2024, incidents more commonly involved roof, ceiling or perimeter entry, with many resulting in nothing being stolen or only limited losses involving assets and computers. In 2025, the methods included more deliberate approaches such as underground tunnelling, wall breaches and cutting into ATMs and safes. The banking industry continues to invest in after hours intrusion detection, stronger protection of roofs, ceilings, safes and ATM rooms, and prompt alarm response. Each incident is assessed to identify lessons that can be used to strengthen existing security controls and improve security standards across bank branches.

Bank Burglary Incidents and Cash Losses

Measure	2024	2025	% Change
Incidents	27	22	**-19%**
Cash Losses	R1 467 620	R2 226 540	**52%**

Bank Burglary Incidents per Sub Type

Incident Sub-Type	Incidents	
	2024	2025
Burglary - Asset	3	2
Burglary - Cash	3	3
Burglary - Computer	6	6
Burglary - Nothing Stolen	15	11
Burglary Total	**27**	**22**

Incidents and Cash Losses per Province

Province	Incidents	
	2024	2025
Eastern Cape	5	1
Free State	4	2
Gauteng	8	9
KwaZulu-Natal	1	0
Limpopo	1	1
Mpumalanga	0	3
Northwest	2	3
Northern Cape	0	1
Western Cape	6	2
Burglary Total	**27**	**22**

In 2025, bank branch burglaries remained concentrated in a small number of provinces. Gauteng recorded the highest number of incidents, while Mpumalanga warrants closer monitoring after increasing from no incidents in 2024 to three incidents in 2025. The Eastern Cape and Western Cape recorded notable declines. Overall, the national reduction was mainly driven by improvements in previously affected provinces, although Gauteng and Mpumalanga remain priority areas for continued monitoring.

International Perspective

Internationally, bank branch burglary remains a persistent physical security risk, although it occurs less frequently than other forms of banking crime.[1] Comparable markets manage this risk through layered security measures, including secure opening and closing procedures, protection of cash and valuables, alarm response, evidence preservation, cameras, locks, vaults and staff training.[1]

In some developed markets, traditional branch robberies have declined, while physical attacks have increasingly shifted towards ATMs, cash servicing points and weaknesses in bank premises.[2, 3] This supports the continued South African focus on stronger branch protection, effective after hours detection, secure safe and ATM room controls, and coordinated incident response.[2, 3]

Risks linked to staff, contractors and service providers also remain important because these individuals may understand branch routines, systems and access points.[3] Branch burglary controls should therefore include appropriate staff conduct, access management and incident reporting measures, in addition to physical security such as alarms, locks and doors.[1, 3, 4]

1 *Electronic Code of Federal Regulations. 2026. 12 CFR 208.61 - Bank security procedures.*

2 *European Banking Federation. 2019. Physical Security Landscape 2019.*

3 *ABA Banking Journal. 2024. Rage against the machine thieves.*

4 *ABA Banking Journal. (2025). The threat from within: Managing insider threat risks.*

BANK ROBBERY

During 2025, the banking sector reported two bank branch robbery incidents, compared to eight in 2024.

Bank Robbery Incidents and Cash Losses

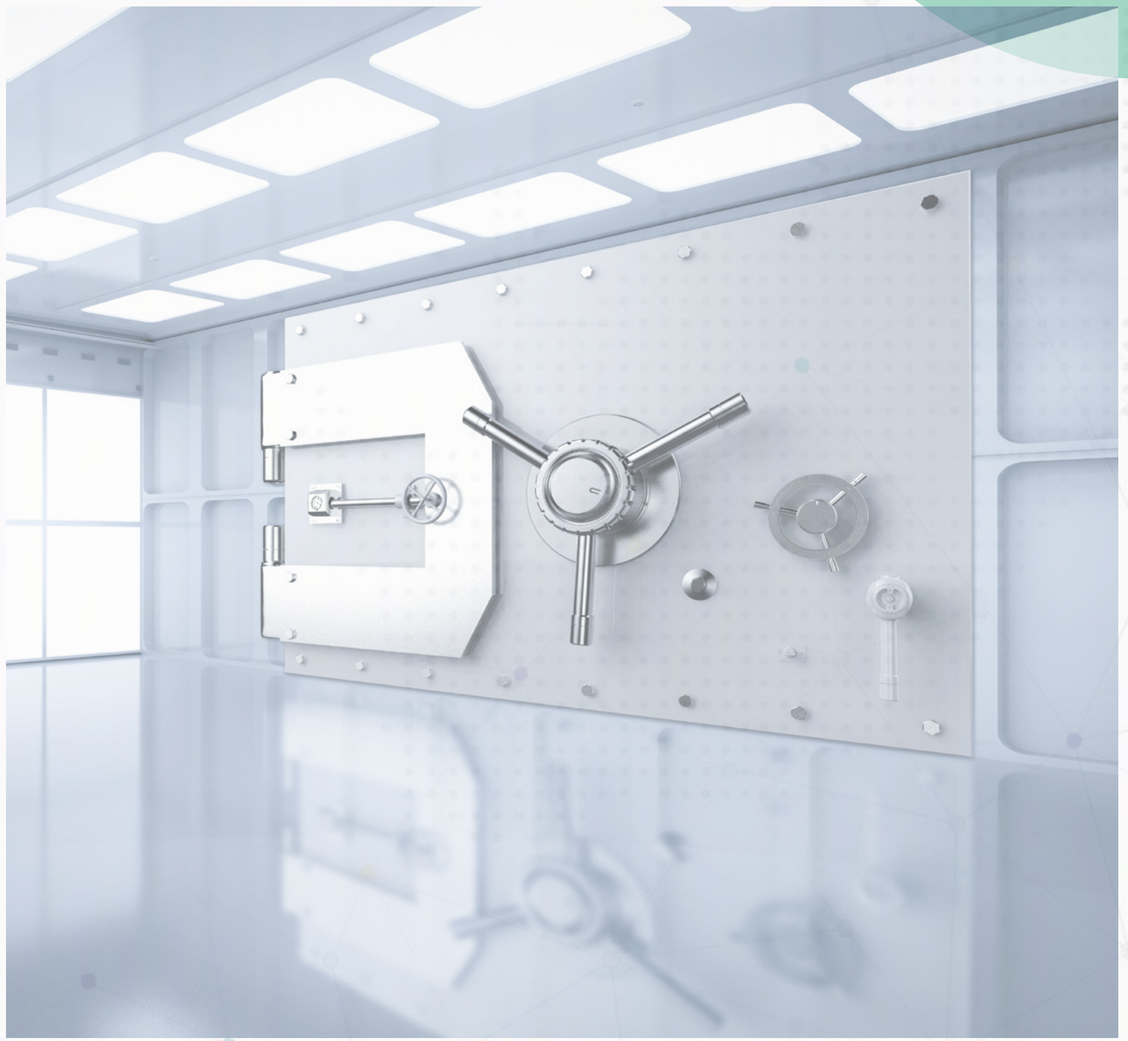
Measure	2024	2025	% Change
Incidents	8	2	**-75%**
Cash Losses	R3 672 357	R630 000	**-83%**

The Eastern Cape incident in 2025 resulted in no reported cash loss, while the Mpumalanga incident accounted for the full **R630 000** loss. Although the lower number of incidents in 2025 is encouraging, the Mpumalanga matter highlights the continued importance of access management and layered security controls within bank branches.

International Perspective

Bank robberies remain at comparatively low levels in mature banking markets, while broader robbery trends have continued to decline.[1, 2] In the United States, the FBI's preliminary 2025 crime data showed that robbery decreased by an estimated **18.5%** from 2024 to 2025, while the FBI also moved to more frequent monthly crime data releases during 2025 to provide more timely trend monitoring.[1, 2] In Italy, the Italian Banking Association (ABI) and OSSIF reported during 2025 that bank robberies continued to decline sharply, with the robbery risk index falling to **0.3** robberies per **100** branches and the ten-year trend showing a reduction of more than **90%**.[3] These 2025 updates support the view that traditional bank branch robberies are being contained through reduced branch cash exposure, improved surveillance, stronger security procedures, staff awareness and closer cooperation between banks and law enforcement.[3, 4]

The international pattern in 2025 also indicates that criminal attention continues to shift from traditional teller-counter robberies toward ATM-related physical attacks, fraud, cash-in-transit risks and vulnerabilities around cash servicing points.[4, 5] South Africa's 2025 bank branch robbery experience therefore aligns with the low incident volumes reported internationally, but the local risk remains important because incidents can still involve planning, intimidation and potential violence. This reinforces the need for strong access management, staff procedures, surveillance, after-hours controls, panic response capability and layered branch security.[1, 3, 4, 5]



1 *Federal Bureau of Investigation. (2026). FBI releases historic early look at annual crime data: First Look 2025 Crime Data.*

2 *Federal Bureau of Investigation. (2025). FBI releases monthly crime and law enforcement data.*

3 *OSSIF / ABI. 2025. Banks and Security (2025) reporting on the continued decline in bank robberies and the reduction in the robbery risk index.*

4 *American Bankers Association. (2025). Physical security resources, robbery deterrence guidance and branch opening process recommended practices.*

5 *American Bankers Association. (2025). ATM crime trends and physical security risks affecting banks and cash service points.*

SABRIC | South African Banking Risk Information Centre

CONTACT US

Siemens Park, 300
Janadel Avenue,
Halfway House, 1685

(+27) 11 847 300

FOLLOW US

YouTube
X (Twitter)
Facebook
Instagram

SabricZA
@Sabric
SabricZA
sabric sa