NATIONAL PAYMENT SYSTEM FRAUD

(10 YEAR FRAUD TREND)

REPORT

13 MARCH 2023

DISCLAIMER

The Bank of Namibia (the Bank) disclaims any responsibility for the manner in which any part of this report may be used. This report was prepared based on the data collected from the National Payment System Participants overseen by the Bank. The data is validated to ensure completeness and accuracy, however, the Bank cannot fully guarantee the accuracy of the data and therefore, accepts no responsibility or liability whatsoever with regard to the information provided in this report.

CONTENTS

1. INTRODUCTION

One of the Bank of Namibia's (the Bank) strategic objectives is to safeguard and maintain financial stability in Namibia. The Bank through its regulatory mandate as the overseer of the National Payment System (NPS) ensures the safety, security and efficiency of the NPS. In this regard, the Bank established an NPS fraud threshold of 0.05%, which is continuously monitored to maintain public trust. In addition, in December 2022 the Bank issued the *Determination of the Operational and Cybersecurity Standards within the National Payment System (PSD-12),* to address the increase in cybersecurity risks and further assist the Payments Association of Namibia (PAN) and industry to curb fraud in the NPS.

The prevalence of fraud in the NPS has been on an increasing trajectory over the years. The payments landscape is ever-evolving and as technology becomes more sophisticated so does criminal fraud. Generally, payments fraud emanates from the use of various payment instruments namely card, electronic funds transfer (EFT), cheque and electronic-money (e-money). The *Payment System Management Act, No.8 of 2003, as amended*, defines a payment instrument as an instrument or process enabling a payer to issue a payment instruction. Cash is however not considered a payment instrument in the NPS, thus the existing payment instruments are card which is categorised between debit, hybrid, and credit; EFT that is split between EFT credits and debits; and e-money.

Common fraud perpetrated in the NPS relate to card, EFT and e-money payment instruments. Card fraud include lost or stolen cards, forged or counterfeit cards, card-not-present payments, and not received issued cards. On the other hand, EFT fraud results through SIM card swopping, denial-of-service attacks and social engineering techniques like phishing, while e-money fraud originates from phone call scams and SIM card swopping. Cash fraud emanates from internal theft and external theft as well as cash counterfeit. Fraud continues to be a persistent issue in the NPS, and the rapid speed of technological advancements create both new opportunities for fraud and demands for effective fraud mitigation initiatives. **This report provides an overview of the fraud committed in the NPS using the various payment instruments inclusive of cash during the period 2013 to 2022.**

2. PAYMENT INSTRUMENT FRAUD BY VOLUMES AND VALUES

2.1 Card Fraud

Figure 1: Overall Card Fraud 2013 to 2022

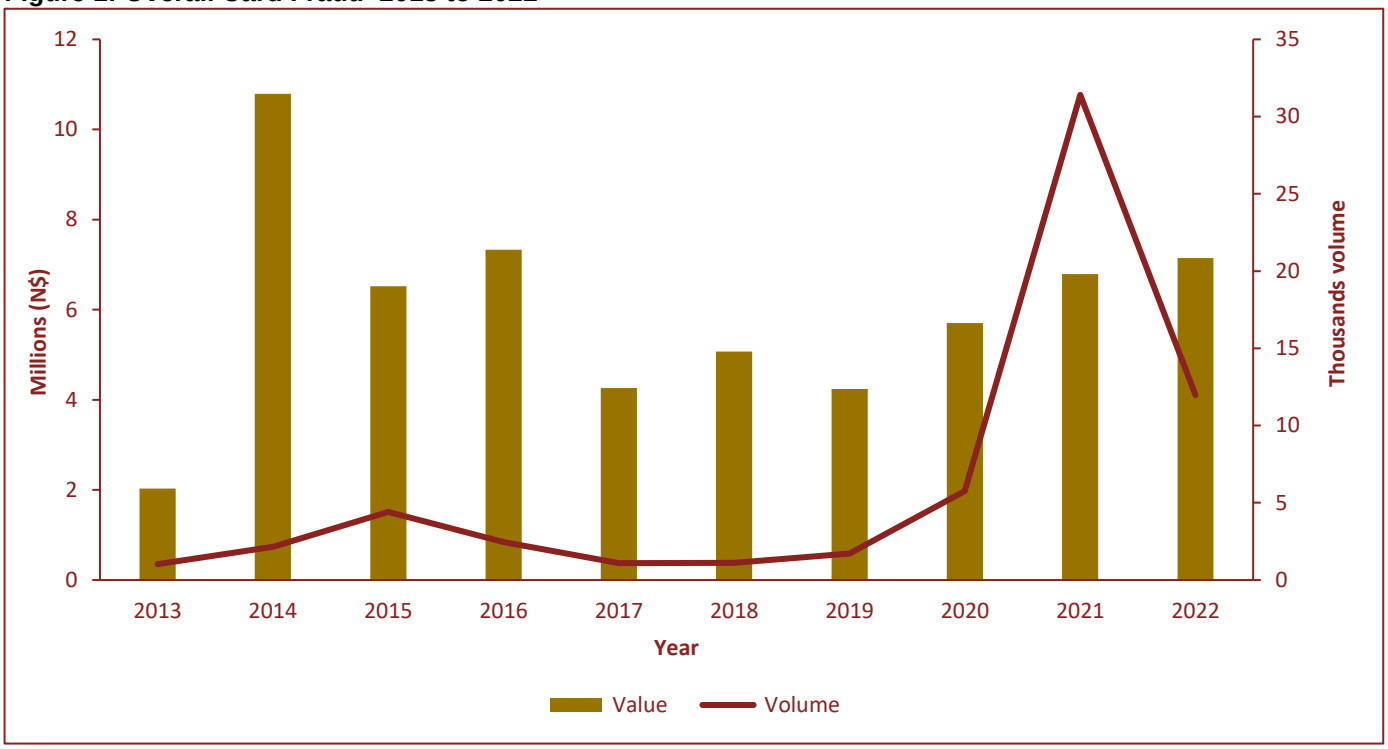


Figure 1 depicts the total fraud committed using the card payment instrument by volumes and values for the period 2013 to 2022. During the period under review card fraud incidents remained relatively low with the exception of 2021 and 2022 that reported 31.4 thousand incidents and 11.9 thousand incidents, respectively. Card fraud incidents in 2021 increased by 25.6 thousand incidents from 5.7 thousand incidents noted in 2020. In 2022, card fraud incidents, however, declined drastically by 19.4 thousand incidents, due to a significant decline in card-not-present incidents. Card-not-present payments fraud occurs when a payment card transaction is made where the cardholder does not or cannot physically present the card at the time of the transaction for the merchant's visual examination. The least card fraud incidents occurred during 2013 (1.02 thousand incidents), 2017 (1.09 thousand incidents) and 2018 (1.1 thousand incidents). In terms of value, card fraud increased during 2014 by N$8.7 million, 2016 by N$813.0 thousand, 2018 by N$811.0 thousand, 2020 by N$1.4 million, 2021 by N$1.0 million and 2022 by N$356.7 thousand. The highest card fraud were observed in 2014 (N$10.7 million), 2016 (N$7.3 million) and 2022 (N$7.1 million), while the lowest card fraud was observed in 2013 (N$2.0 million). Card fraud increased sharply during 2014 by N$8.7 million, due to increased lost or stolen, and forged or counterfeit card fraudulent activities. The period under review recorded a total of 63.0 thousand card fraud incidents valued at N$59.8 million.

PANEL A: Card Fraud category by volumes and values 2013 to 2022

Figure 2: Card Fraud category by volumes

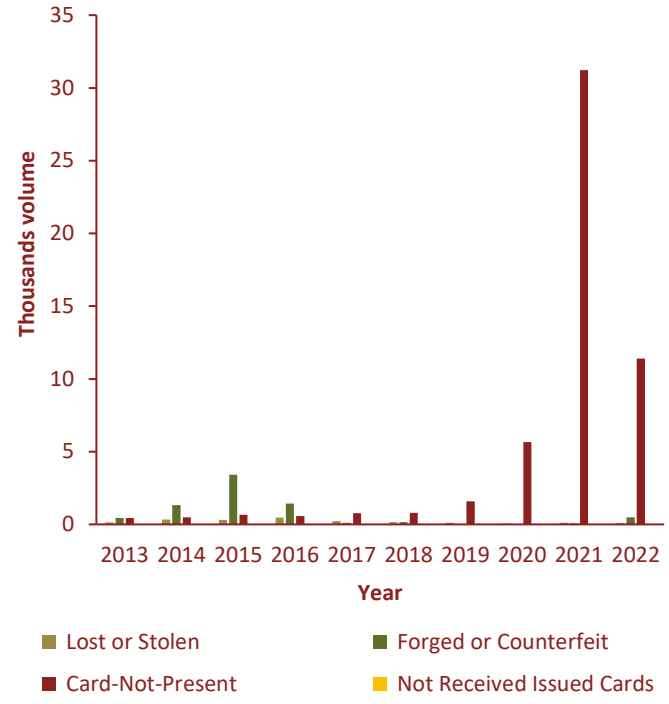
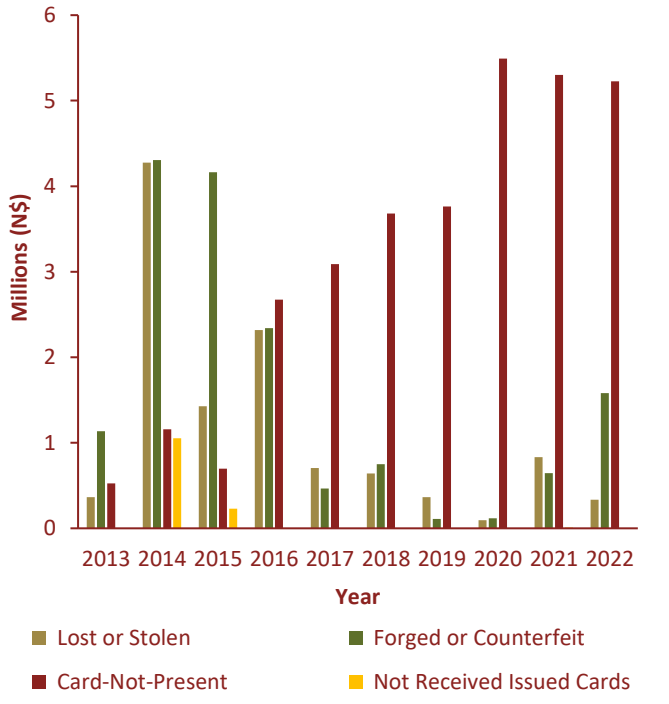


Figure 3: Card Fraud category by values



Panel A presents the common card fraud types by volumes and values for the period 2013 to 2022. Figure 2 shows that most card fraud incidents reported in 2021 stemmed from card-not-present payment incidents. The surge in card-not-present payment incidents was attributed to the rise in card usage during the COVID-19 pandemic and inadequate online card security measures. During the review period, the least card fraud incidents originated from lost or stolen card, forged or counterfeit cards, and not received issued card. From a value standpoint, Figure 3 depicts that the highest card-not-present payment losses were noted during 2020 (N$5.4 million), 2021 (N$5.3 million) and 2022 (N$5.2 million). Similarly, 2014 recorded the highest card fraud losses for forged or counterfeit cards valued at N$4.3 million, lost or stolen card valued at N$4.2 million, and not received issued card valued at N$1.0 million. When a criminal skims or copies the data held on the magnetic stripe of a legitimate card and uses this data to create a fake plastic card which contains the real card details is referred to as forged or counterfeit card fraud. Moreover, lost or stolen card fraud occurs when fraudster uses a payment card obtained without the knowledge of the lawful owner, following card theft or loss. The period under review reported 1.9 thousand lost or stolen card incidents valued at N$11.3 million, 7.4 thousand forged or counterfeit incidents valued at N$15.6 million, 53.6 thousand card-not-present payment incidents valued at N$31.6 million, and 16 not received issued card incidents valued at N$1.2 million.

2.2 EFT Fraud

Figure 5: Overall Domestic EFT Fraud 2013 to 2022

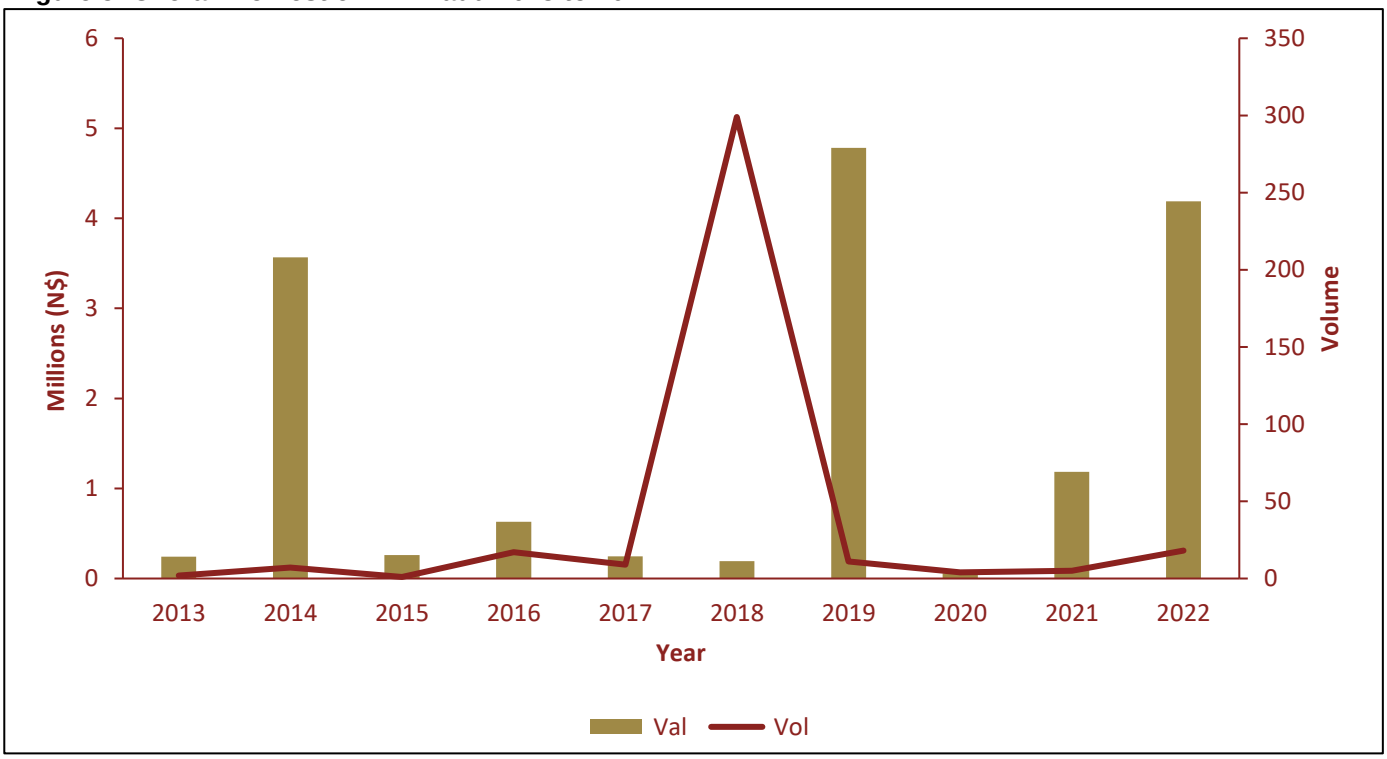


Figure 5 shows the overall domestic EFT fraud committed during the period 2013 to 2022. The period under review recorded incredibly low EFT fraud incidents with the exception of 2018 with 299 incidents, primarily due to phishing attacks. Phishing is an online banking fraud method used to deceitfully obtain personal information such as passwords, identity numbers and credit card details by sending emails that look like they come from trusted sources like banks, service providers etc. During 2018, EFT fraud increased sharply by 290 incidents, but further declined by 288 incidents during 2019 as a result of a significant drop in phishing attacks. This translates into a decline of 96.3% that could be attributed to the fraud awareness videos launched by PAN with the assistance of Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) to educate the public. The least EFT fraud incidents occurred in 2015 with only 1 incident noted. From a value perspective, the highest EFT fraud losses were reported in 2019 (N$4.7 million), 2022 (N$4.2 million), 2014 (N$3.5 million) and 2021 (N$1.1 million), while 2020 recorded the least funds lost valued at N$56.0 thousand. A significant increase of N$4.5 million was noted between 2018 and 2019 mainly due to phishing attacks, but declined tremendously by N$4.7 million between 2019 and 2020, because of a decrease in SIM card swop and phishing incidents. Despite the decline noted in 2020, EFT fraud increased by N$1.1 million in 2021 and further increased by N$3.0 million in 2022, mainly due to increased phishing attacks. During the period 2013 to 2022 a total of 373 EFT fraud incidents were reported valued at N$15.3 million.

Panel B: EFT Fraud category by volumes and values 2013 to 2022

Figure 6: EFT Fraud category by volumes

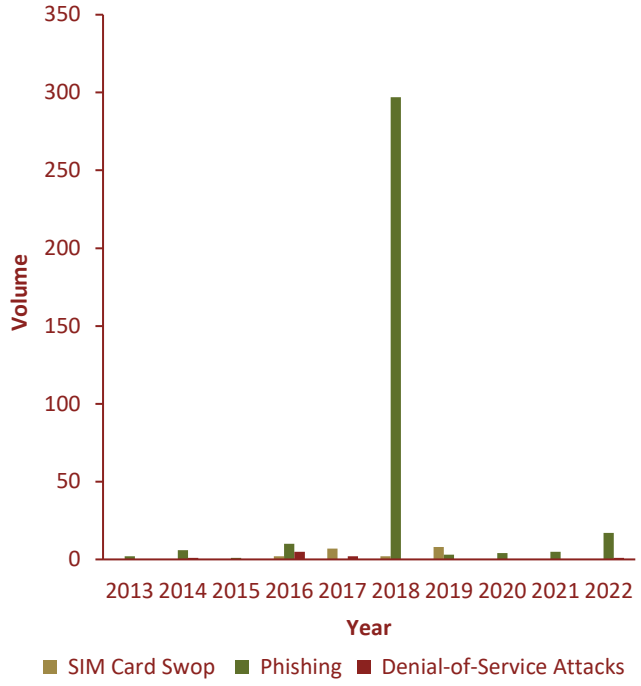
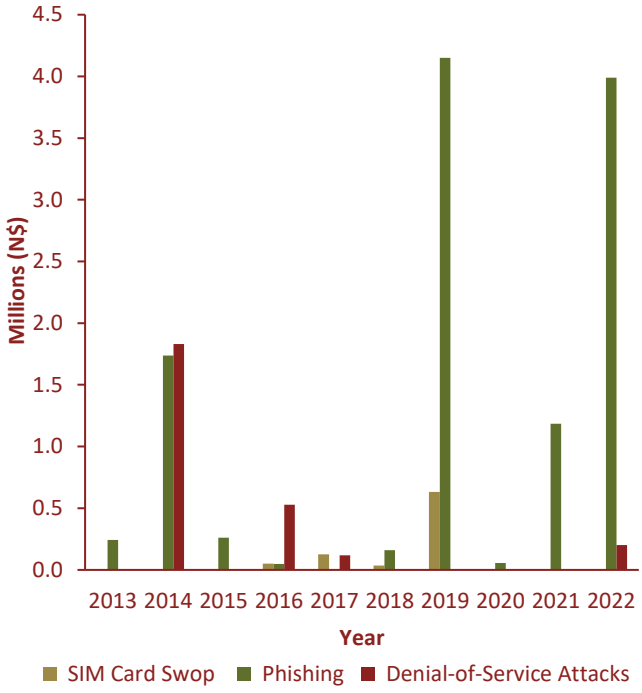


Figure 7: EFT Fraud category by values



Phishing attacks continued to be more frequent from both a volume and value standpoint as shown in Panel B. Figure 6 indicates that most EFT fraud incidents occurred in 2018 with 297 phishing incidents reported. SIM card swop incidents with 8 incidents reported recorded the most incidents during 2019. SIM card swop is a form of fraud where criminals request your cell phone service providers to transfer your existing cell phone number onto a new SIM card by pretending to be a client or pretending to act on the client's behalf. The period under review recorded a total of 19 SIM card swop incidents, 345 phishing incidents and 9 denial-of-service incidents, hence the least EFT fraud originated from denial-of-service attacks. In terms of the value, Figure 7 shows that phishing attacks recorded the highest EFT fraud value during 2019 (N$4.1 million), 2022 (N$3.9 million), 2014 (N$1.7 million) and 2021 (N$1.1 million). In regard to denial-of-service attacks the highest value of N$1.8 million was noted in 2014. Denial-of-service attack is any type of attack where attackers attempt to prevent legitimate users from accessing a service. In the same vein, during 2019, SIM card swop recorded the highest EFT fraud valued at N$632.5 thousand. For the period under review, phishing attacks accounts for 92.5% and 77.0% of the total EFT fraud incidents and value, respectively, while the remainder comprised of denial-of-service attacks and SIM card swopping.

2.3 E-money Fraud

Figure 9: Overall E-money Fraud[1] 2015 to 2022

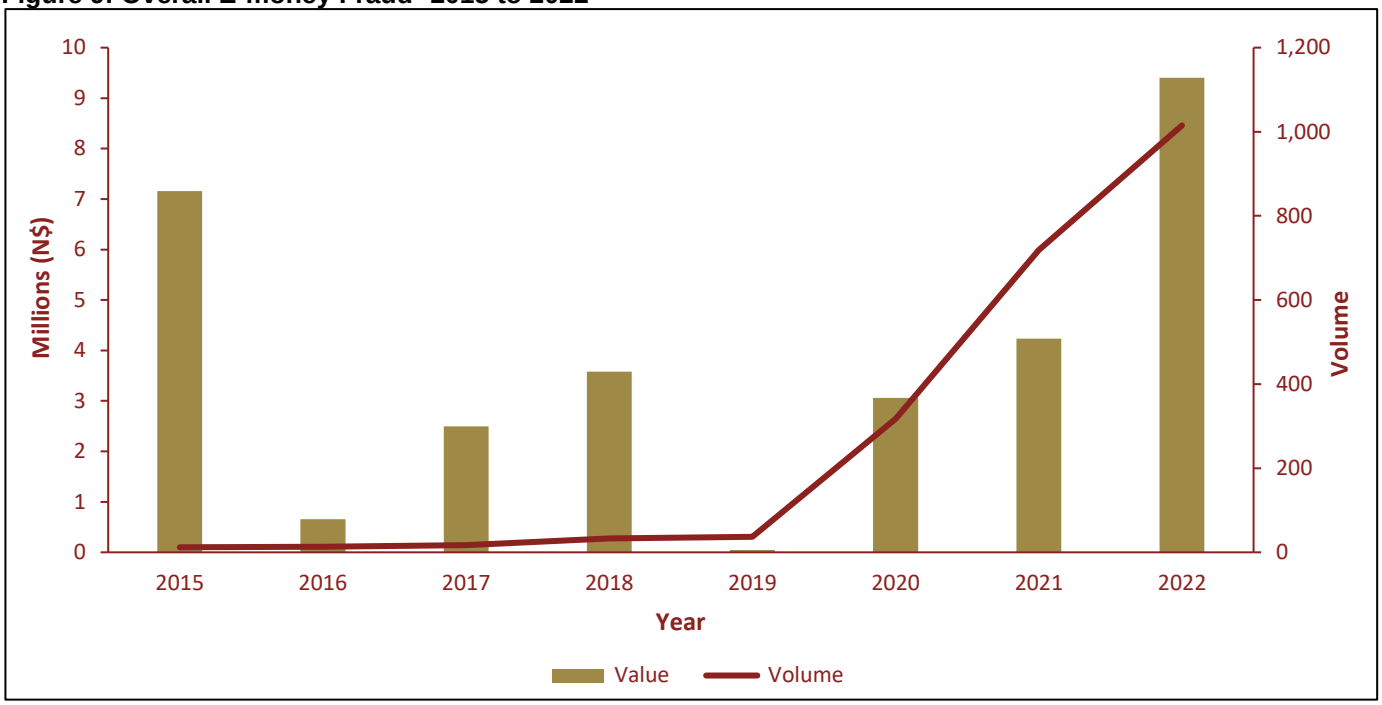


Figure 9 depicts e-money fraud by volumes and values for the period 2015 to 2022. E-money fraud incidents remained fairly low between 2015 to 2019, however began to increase significantly during 2020, 2021 and 2022. Most e-money fraud incidents occurred during 2022 with 1.0 thousand incidents reported where customers were exploited through phone call scams, and fraudsters manged to obtain their personal information. The increase in e-money fraud during 2020 and 2021 could be attributed to changes in consumer behaviour and the spread of COVID-19, as lockdown regulations prompted various entities to use e-money schemes as the preferred payment method for the disbursement of funds to recipients. The least e-money fraud incidents occurred during 2015 (12 incidents), 2016 (13 incidents) and 2017 (17 incidents). From a value standpoint, the highest e-money fraud was recorded in 2022 valued at N$9.4 million followed by 2015 valued at N$7.1 million and 2021 valued at N$4.2 million. E-money fraud increased remarkably during 2017 by N$1.8 million, N$1.0 million in 2018, N$3.0 million in 2020, N$2.0 million in 2021 and N$5.2 million in 2022. On the contrary, e-money fraud also declined during 2016 and 2019 by N$6.4 million and N$3.5 million, respectively. The least e-money fraud was reported in 2019 with a value of N$48.8 thousand, because of SIM card swop incidents. During the period under review, e-money fraud recorded a total of 2.1 thousand incidents valued at N$30.6 million.

[1] No e-money fraud was noted during 2013 to 2014.

Panel C: E-money Fraud category by volumes and values 2015 to 2022

Figure 10: E-money Fraud category by volumes

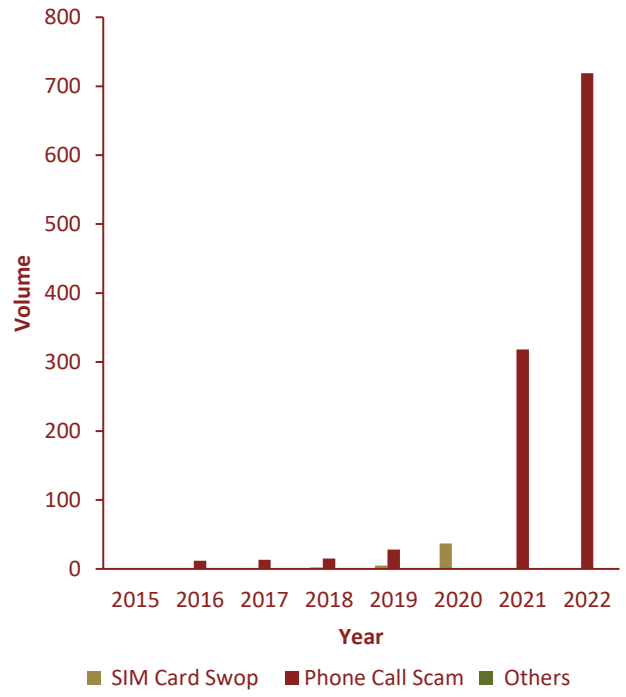
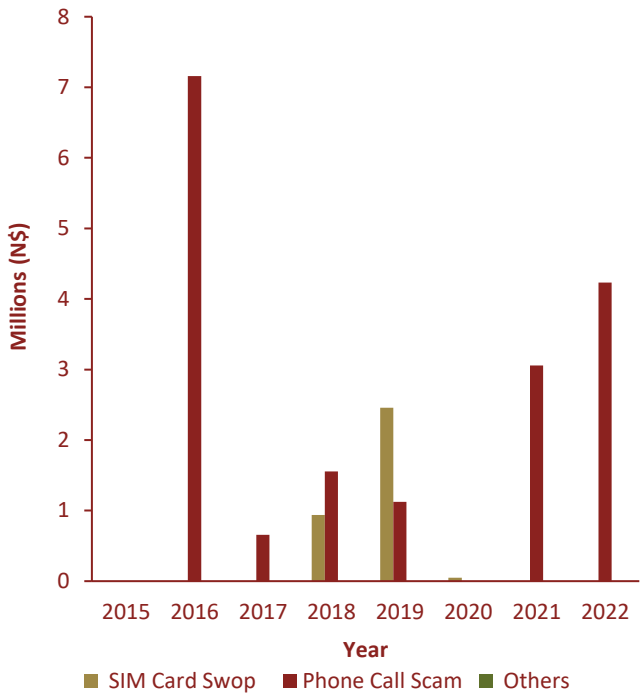


Figure 11: E-money Fraud category by values



Panel C reveals that phone call scams in comparison to SIM card swop incidents continued to be prevalent during 2015 to 2022 with the exception of 2019. Figure 10 shows that phone call scams recorded the most incidents during 2022 (1.0 thousand incidents) and 2021 (719 incidents). The least phone call scam incidents were reported in 2015, 2016 and 2017 with 12 incidents, 13 incidents and 15 incidents reported, respectively. Phone call scams fraud happens when personal information of a consumer is solicited by the fraudsters and typically involves technical support calls, lottery scams, and bank fraud calls. SIM card swop on the other hand recorded the highest incidents during 2019 with 37 incidents reported, while the least incidents were observed in 2017 (2 incidents) and 2018 (5 incidents). The period under review reported 45 SIM card swop incidents and 2.1 thousand phone call scam incidents. In terms of value, Figure 11 indicates that phone call scam fraud recorded the highest e-money fraud valued at N$9.3 million in 2022, N$7.1 million in 2015, N$4.2 million in 2021 and N$3.0 million in 2020. The least e-money fraud phone as a result of phone call scams was recorded in 2016 valued at N$658.2 thousand. In terms of SIM card swop incidents the highest value of N$2.4 million was noted in 2018, while the least was reported in 2019 (N$48.8 thousand). During the review period, phone call scam incidents and SIM card swopping incidents resulted in a total loss of N$3.4 million and N$27.1 million, respectively.

2.4 Cash Fraud

Figure 13: Overall Cash Fraud 2013 to 2022

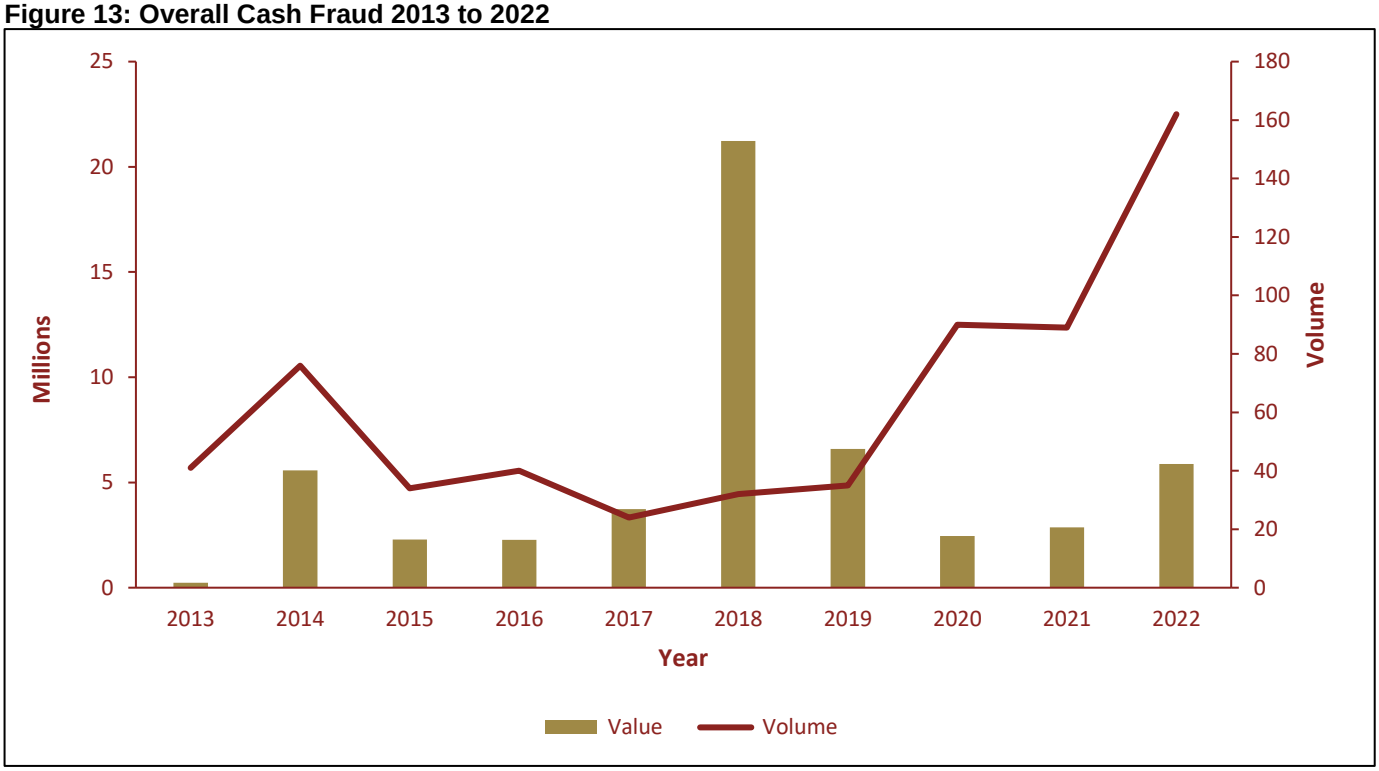


Figure 13 shows the overall cash fraud committed by volumes and values for the period 2013 to 2022. Cash fraud incidents increased during 2014, 2016, 2018 and 2022 for the period under review. The highest cash fraud incidents were reported in 2022 with 162 incidents, followed by 2020 with 90 incidents and 2021 with 89 incidents. Cash counterfeit is an illegal act of reproducing legal tender currency for the sole purpose of using it as legal tender for the purchase of goods and service in the economy. The least cash fraud incidents were noted during 2017 with 24 incidents reported, mainly due to external theft a form of fraudulent practice attributed to external sources, such as robbery. From a value standpoint, the highest cash fraud occurred in 2018 valued at N$21.2 million. Cash fraud increased drastically by N$5.3 million in 2018 and N$17.4 million in 2014. Cash fraud, however, declined considerably by N$15.3 million between 2018 and 2022 , as a result of improvement in controls to minimise cash theft (internal and external). The least cash fraud was recorded during 2013 with a value of N$231.9 thousand. During the period under review, cash fraud reported a total of 623 incidents valued at N$15.3 million.

Panel D: Cash Fraud category by volumes and value 2013 to 2022

Figure 14: Cash Fraud category by volumes

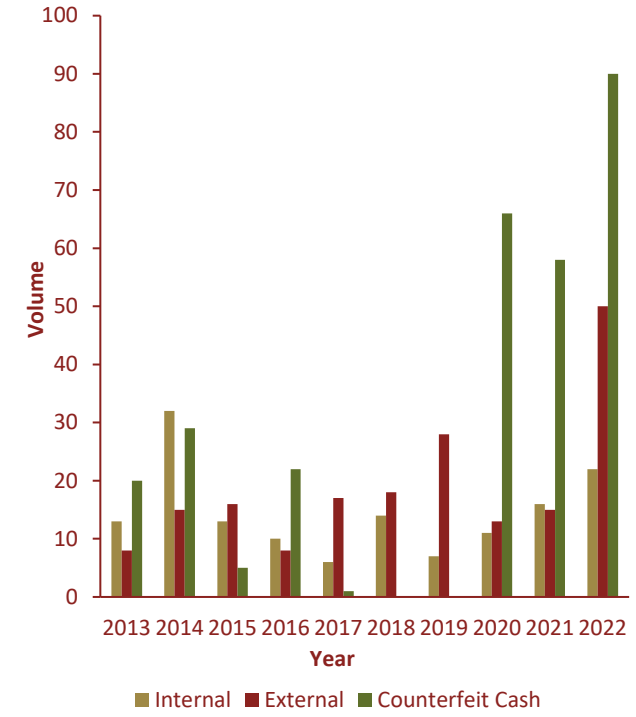
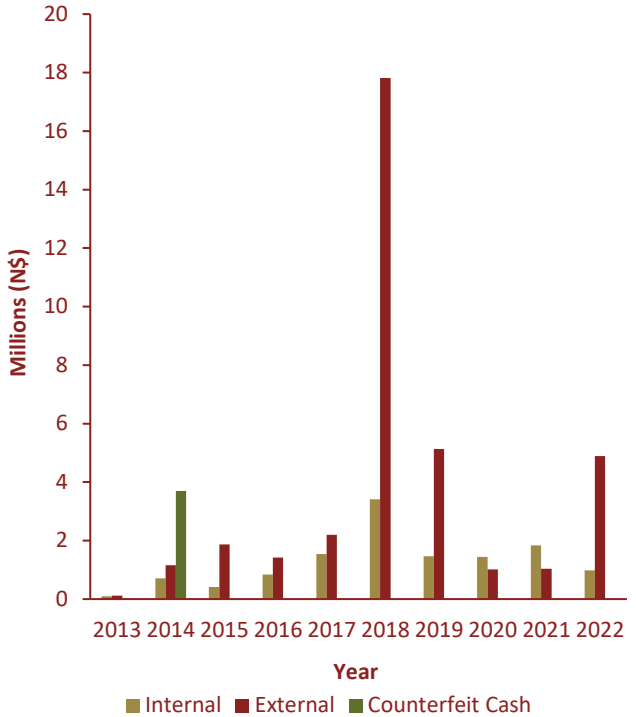


Figure 14: Cash Fraud category by value



Panel D shows that most cash fraud incidents emanated from cash counterfeits, while external theft incidents resulted in high value losses. Figure 14 depicts that cash counterfeits resulted in high cash fraud incidents during 2022 (90 incidents) and 2020 (66 incidents). Likewise, internal cash theft (22 incidents) and external cash theft (50 incidents) reported the most incidents during 2022. Cash fraud reported a total of 623 incidents of which 46.7% originated from counterfeit incidents, 30.2% from external theft incidents and 23.1% from internal theft incidents. From value perspective, Figure 15 shows that the highest cash fraud recorded in 2018 valued at N$17.8 million resulted from external theft incidents. Equally, during 2018 internal theft incidents recorded the highest value of N$3.4 million. Internal theft fraud results from embezzlement or illegal activity by employees such as stealing money from their employers. Cash counterfeit on the other hand recorded the highest cash fraud during 2014 with a value of N$3.7 million. During the review period total cash fraud reported a total value of N$53.1 million comprising of external theft incidents valued at N$36.6 million, internal theft incidents valued at N$12.7 million and counterfeit incidents valued at N$3.7 million.

3. SNAPSHOT OF THE NPS FRAUD

PANEL E: Share of NPS Fraud by volumes and values

Figure 17: Total NPS Fraud share by volumes

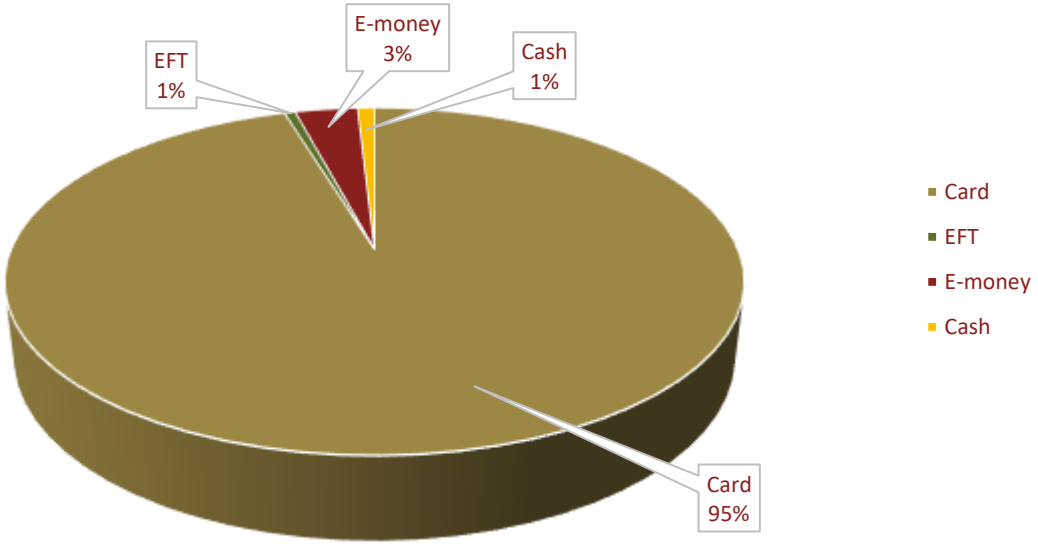
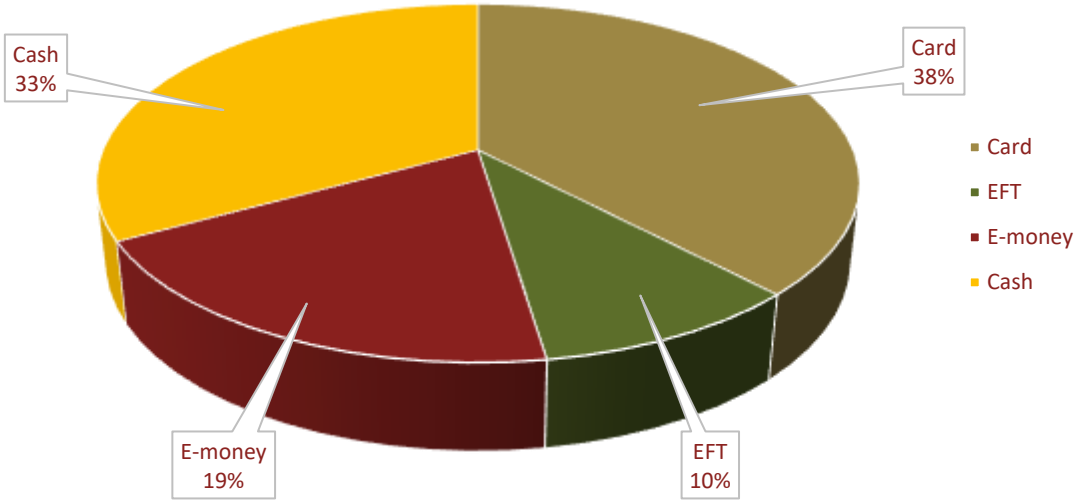


Figure 18: Total NPS Fraud share by values



Panel E presents the total share of NPS fraud by volumes and values for the various payment instruments inclusive of cash for the period 2013 to 2022. As shown in Figure 17 fraud incidents in the NPS was predominately due to the card payment instrument with a share of 95%, followed by e-money with 3%, while the least incidents resulted from the EFT and cash with 1% each. Likewise in terms of the value as presented in Figure 18 the share of the card payment instrument was the highest with 38% but followed by cash fraud with 33% and e-money with 19% and the least was EFT with 10%.

4. CONCLUSION

The total fraud in the NPS inclusive of cash fraud was 66.2 thousand incidents valued at N$158.9 million for the period 2013 to 2022. During the period under review, card fraud recorded 63.0 thousand incidents valued at N$59.8 million, e-money recorded 2.1 thousand incidents valued at N$30.6 million, EFT recorded 373 incidents valued at N$15.3 million and cash fraud reported 623 incidents valued at N$53.1 million. Generally, majority of the card fraud incidents, e-money fraud incidents and EFT fraud incidents emanated from card-not-present payments, phone call scams and phishing attacks, respectively.

PAN along with industry are constantly educating the public and implementing initiatives to curb fraud in the NPS. The industry strengthened and implemented efficient authentication controls in the EFT environment. In terms of card, the industry advanced card security through the adoption and compliance to EuroPay, Master Card and Visa and Payment Card Industry Data Security Standards. In addition, the industry also made significant investments over the years to develop new card products and to provide additional layers of security for card transactions. Equally, introduced 3D secure protocols to increase the security measures around e-commerce transactions in order to prevent card fraud related to card-not-present transactions. In regard to e-money the industry continues to create awareness and educate the public on e-money related fraudulent activities. Despite the efforts by PAN and the industry fraudsters are endlessly finding new ways to compromise payment instruments, but the industry and PAN continue creating and implementing new innovations to combat fraudsters in order to ensure that the NPS remains safe, efficient and secure for the public.