
# BANKS & SDI FRAUD REPORT

This report is a definitive overview of various attempted or perpetuated fraudulent activities recorded by Ghana's banks and SDIs. It presents the industry position for the period January 01 2020 to December 31 2020

## 2020

## TRENDS & STATISTICS

FINANCIAL SYSTEM STABILITY DEPARTMENT

# THE 2020 BANKING INDUSTRY FRAUD REPORT

## EXECUTIVE SUMMARY

In 2020 many routine activities of institutions including financial transactions that usually would have been undertaken in-person were conducted online. Customers who were not used to digital/electronic methods of making financial transactions were compelled to use them. Consequently, some sections of the banking sector were exposed to heightened levels of fraud related risk, due to the increased patronage of electronic/digital products and services. The emergence of the COVID-19 pandemic propelled the use of digital/electronic modes of transacting business, leading to a higher exposure to fraud.

The year 2020 recorded a marginal increase in reported fraud incidents with a minimal decrease in losses. The reduction in losses was mainly due to a reduction in the rate of success for most fraud types. A total case count of 2,670 cases were recorded in the year 2020, as compared to 2,311cases in 2019 (refer to Table 2 below).

The Reported value of fraud for 2020 was GH¢1.0 billion, as compared to GH¢115.51million recorded in 2019. (Refer to Table 3). The notable increase in the value reported was as a result of high values recorded in attempted correspondent banking fraud (forgery of SWIFT advice). Even though the banking sector did not suffer any losses from any of the correspondent banking fraud attempts, it posed a reputational risk to some banks, whose staff were found culpable in two of the three reported incidents.

Losses incurred as a result of fraud for 2020 stands at GH¢25.40 million, as compared to an estimated loss of GH¢33.44 million in 2019, representing a 24.0% decrease. (Refer to Table 4 below).

The COVID-19 pandemic resulted in a surge in the use of digital/electronic platforms for financial transactions, considerably. In an effort to contain the spread of the virus, financial institutions encouraged customers to take full advantage of the various digital products and services available, to execute financial transactions. The surge in usage led to an increase in the incidence of fraud related to digital/electronic products and services and consequently, an increase in losses emanating from products such as E-Money and ATM/Card fraud.

Submission of fraud returns for 2020, recorded a slight improvement. The banks continued to maintain a 100% rate of submissions and the rural and community banking sector recorded a remarkable increase of 75% in the rate of submissions due to administrative sanctions issued against non-submitting banks in the first half of the year (Refer to table 1 and 2 below). The submission rate across the SDIs will improve marginally if reporting institutions are adjusted to exclude the distressed institutions. The year 2020 recorded 26.4% decrease in the success rate of fraud attempted. Some fraud types experienced a significant increase in the rate of success, as compared to 2019, whiles others recorded a remarkable decrease in their rate of success, in comparison with 2019. Fraud types such as ATM/POS fraud, impersonation and remittance fraud recorded significant increases in their rate of success for the period under review. (Refer to Figure 3 below).

ATM/POS related fraud accounted for 32.2% of total fraud related loss incurred in 2020 and recorded the highest loss value of GH¢8.19 million in 2020, as compared to GH¢1.26 million recorded in 2019, representing a 548.1% increase in year on year terms. (Refer to Table 4 & 5 below). The COVID-19 pandemic forced bank customers to use alternative channels for payments and bank services. Poor personal safety perception and inadequate customer sensitization by banking institutions may be the cause of the increase in the ATM/POS fraud type.

Staff involvement in the commission of fraud also experienced a significant increase, especially suppression of cash. 56% of reported fraud cases and 93% of reported cash suppression cases involved staff of the reporting institutions. (Refer to figure 2).

Data recorded over the years shows a persistent trend of staff involvement in fraud. Despite the numerous notices of caution sounded out to the banking industry, in almost every fraud report issued since 2017, the phenomenon continues to increase. The steady rise in this phenomenon generally could be attributed to the use of poorly remunerated temporary staff, who undergo limited background checks, for sensitive tasks and a lack of corporate governance systems that helps to ensure accountability and fairness and transparency.

E-Money fraud is beginning to show a steady rise in the count of reported incidents. E-Money related loss accounted for 4.1% of the total fraud related loss incurred in 2020, as compared to a rate of 1.1% recorded in 2019. The proportion of E-Money related fraud incidents reported rose from 0.6% in 2019 to 4.7% in 2020. (Refer to tables 5 and 6).

Key recommendations to help fight current fraud trends include consumer education on the safe usage of digital/electronic products, the improvement of KYC information gathered by mobile money operators (MMOs), and the acquisition of transaction monitoring systems by MMOs to help monitor suspicious transactions.



## 1.0 INTRODUCTION

The Bank of Ghana, as part of its mandate to ensure price stability, contribution to financial stability, and ensuring sound payment systems examines current and past fraud trends in the banking sector as well as the modus operandi utilized by

perpetrators, with the aim of making recommendations to help curb the incidence of fraud in the banking sector.

The banking sector has become more susceptible to fraud due to the increased use of innovative emerging technologies for business transactions. 2020 recorded a marginal increase in reported fraud incidents and a marginal decrease in losses incurred.

In 2020, the industry reported a total fraud value of GH¢1.0 billion compared to GH¢115.5 reported in 2019. The notable increase in the reported fraud value is as a result of high values recorded in attempted corresponding banking fraud.

## 2.0 COMPARATIVE ANALYSIS OF SUBMISSIONS

Banks, rural and community banks, savings and loans and finance houses recorded improvements in their rate of submissions over the last few years. The rate of submissions in the banking sector, has improved from 86.0% in 2017 to 100.0% in 2019 and 2020. The rural and community banking sector has improved the rate of its submissions from 20.1% in 2017 t0 75.0% in 2020. Savings and loans companies and finance houses recorded a marginal increase in their rate of submissions from 16.7% in 2017 to 36.1% in 2020. Table 1 below shows a comparative analysis of the rate of submissions per sector over a four-year period.



**Table 1: Institutional submissions per sector**

| | Commercial Banks | | | | Rural and Community Banks | | | | Saving & Loans/ Finance Houses | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2017 | 2018 | 2019 | 2020 | 2017 | 2018 | 2019 | 2020 | 2017 | 2018 | 2019 | 2020 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Total Number of Institutions Per Sector** | 36 | 30 | 23 | 23 | 139 | 134 | 134 | 144 | 60 | 60 | 60 | 36 |
| **Number of Reporting Institutions** | 31 | 28 | 23 | 23 | 28 | 34 | 49 | 108 | 10 | 10 | 11 | 13 |
| **Proportion of institutions that submitted Reports** | 86.1 | 93.3 | 100.0 | 100.0 | 20.1 | 25.4 | 36.6 | 75.0 | 16.7 | 16.7 | 18.3 | 36.1 |



## 3.0 INCIDENCE OF FRAUD IN 2020

The Bank of Ghana recorded a total of 2,608 incidents of fraud as compared to 2,311 fraud cases reported in 2019, representing a year-on-year increase of 12.9%. Banks and Specialized Deposit-Taking Institutions regulated by the Bank of Ghana are required to submit fraud returns as and when they record incidents of fraud and also, a "Nil Report" if they do not record any incident at the end of a particular month.

Table 2 below shows the total count of fraud incidents reported in 2020/2019. 2020 recorded a total of 2,670 fraud reports, as compared to 2,311 fraud reports filed in 2019, representing a year-on-year increase of 15.5% in the number of fraud returns submitted to the Bank. Quite a few fraud types recorded increases in 2020. The most significant fraud types recorded in 2020, with respect to incidence and/or loss to the banking sector are:

- Fraudulent withdrawals
- E-Money Fraud
- ATM/POS Fraud

Fraudulent Withdrawals recorded the highest rate of increase in the year under review. Fraudulent Withdrawals increased from 16 cases in 2019 to 177 cases in 2020 representing an increment of 1,006.3%. E-Money Fraud also recorded 64 cases in 2020, as compared to 14 cases recorded in 2019, representing an increase of 357.1% in year-on-year terms. ATM/POS Fraud recorded 168 cases in 2020, as compared to 110 cases recorded in 2019, representing a 52.7% increase in year-on-year terms.

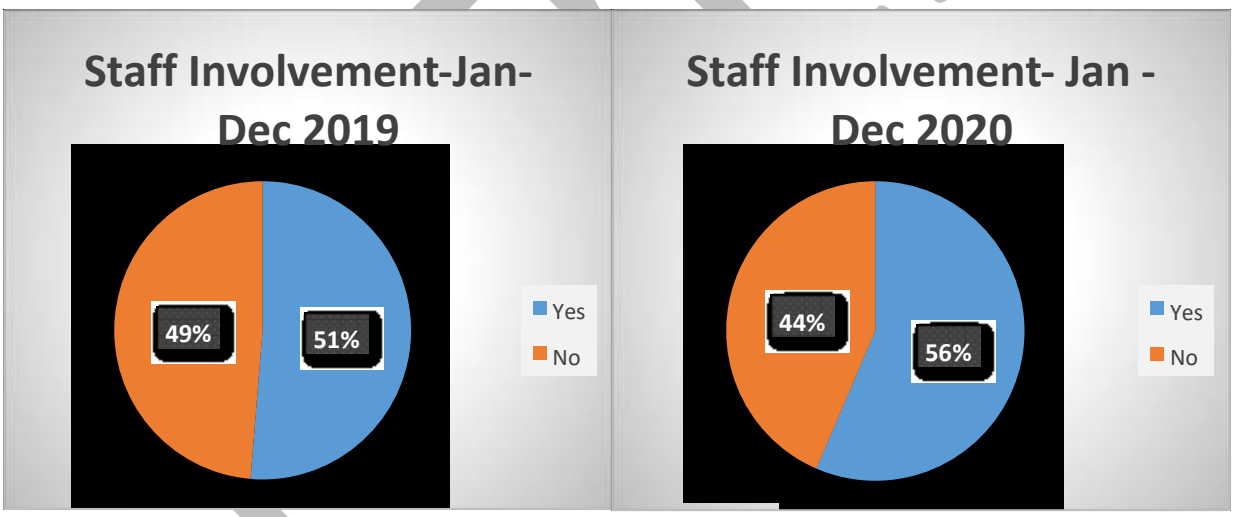
**Table 2 – Count of Fraud Cases**

| Fraud Type | January to December 2019 | January to December 2020 | Y-o-Y Change in 2020 (%) |
|---|---|---|---|
| Suppression | 1774 | 1958 | 10.37 |
| Fraudulent Withdrawals | 16 | 177 | 1,006.25 |
| ATM POS | 110 | 168 | 52.73 |
| Forgery and manipulation of documentation | 157 | 151 | (3.82) |
| e-money | 14 | 126 | 800.00 |
| Cyber - email fraud | 112 | 28 | (75.00) |
| Lending/credit fraud | 36 | 18 | (50.00) |
| Cheque Fraud | 40 | 16 | (60.00) |
| Remittance | 8 | 10 | 25.00 |
| Others | 29 | 9 | (68.97) |
| Burglary | 7 | 6 | (14.29) |
| Impersonation | 8 | 3 | (62.50) |
| Total | 2311 | 2670 | 15.5 |

## 4.0 STAFF INVOLVEMENT

56.0% of fraud incidents reported in 2020 indicated the involvement of staff members of the reporting institutions, as compared to 51.0% of staff involvement reported in 2019. This may be a consequence of the absence of corporate governance structures in some sections of the banking sector, resulting in the lack of accountability and transparency in their activities. Suppression of Deposits accounted for 73.3% of all fraud incidents reported in 2020 and 76.8% of all fraud incidents reported in 2019. Suppression recorded the highest rate of staff involvement. 78.6% of all cash suppression cases reported in 2020, indicated the involvement of staff. Figure 1 below shows the percentage of staff involvement reported for 2019 and 2020.

**Figure 1 STAFF INVOLVMENT**




## 5.0 REPORTED AND SUCCESSFUL FRAUD VALUES

2020 recorded a significant increase in the value of reported cases for the year under review. The total value of reported cases for 2020 amounted to approximately GH¢1.09 billion, as compared to a reported value of GH¢115.51 million recorded in 2019, representing an increase of 773.6% in value of reported cases. The significant increment in reported values is as a result of increased

values in attempted correspondent banking fraud. In some instances, single incidents reported values as high as €100,000,000. Even though attempted fraud values increased significantly, loss incurred through fraud reduced by 24.0%. Table 3 below shows attempted, recovered and loss values for 2019 and 2020.

**Table 3 – Attempted, Recovered and Loss Fraud Values**

| | Jan - Dec 2019 | | | Jan - Dec 2020 | | | Percentage Change in Loss Values (%) |
|---|---|---|---|---|---|---|---|
| Fraud Type | Attempted Amount (GH¢000) | Recovered Amount (GH¢000) | Successful/ Loss Amount (GH¢000) | Attempted Amount (GH¢000) | Recovered Amount (GH¢000) | Successful/ Loss Amount (GH¢000) | |
| ATM POS | 10,962.2 | 9,698.3 | 1,263.9 | 8,420.5 | 229.1 | 8,191.4 | 548.1 |
| Burglary | 709.3 | 24.0 | 685.3 | 1,354.6 | - | 1,354.6 | 97.7 |
| Cheque Fraud | 3,084.2 | 688.9 | 2,395.3 | 6,106.8 | 5,639.3 | 467.5 | (80.5) |
| Cyber - email fraud | 50,542.0 | 36,230.0 | 14,312.0 | 273,880.6 | 272,824.5 | 1,056.1 | (92.6) |
| E-money | 592.6 | 218.2 | 374.4 | 1,926.0 | 877.8 | 1,048.1 | 180.0 |
| Forgery and manipulation of documentation | 37,283.2 | 32,873.9 | 4,409.3 | 8,552.0 | 2,043.3 | 6,508.7 | 47.6 |
| Fraudulent withdrawals | 1,532.2 | 188.6 | 1,343.5 | 3,015.4 | 2,130.7 | 884.7 | (34.2) |
| Impersonation | 687.6 | 591.6 | 96.0 | 62.9 | 3.3 | 59.5 | (38.0) |
| Lending/credit fraud | 1,401.9 | 218.3 | 1,183.6 | 680.1 | 53.8 | 626.3 | (47.1) |
| Others | 3,547.9 | 278.4 | 3,269.5 | 700,980.0 | 698,213.4 | 2,766.6 | (15.4) |
| Remittance | 118.9 | 80.4 | 38.5 | 81.0 | 28.9 | 52.1 | 35.3 |
| Suppression | 5,054.8 | 977.0 | 4,077.7 | 4,094.1 | 1,700.1 | 2,394.0 | (41.3) |
| Total | 115,516.6 | 82,067.6 | 33,449.0 | 1,009,153.9 | 983,744.3 | 25,409.6 | (24.0) |

ATM/POS fraud recorded the highest reported loss value of approximately GH¢ 8.20 million in 2020, as compared to an approximate loss value of GH¢ 1.26 million recorded in 2019. This represents a 548.0 % increase in losses in year-on-year terms. Most of these losses are as a result of card related fraud. The emergence of the COVID-19 pandemic in 2020 led to an increase in the usage of electronic payment systems. E-money fraud also recorded a significant increase in loss value. Loss incurred through E-money fraud increased from approximately GH¢ 0.37 million in 2019 to an estimated GH¢ 1.04 million in 2020, representing a 180.0% percentage increase. This upsurge may also be a result of an increase in use of E-Money services due to the COVID–19 pandemic. Burglary also recorded a considerable increase in reported and loss values for 2020 as compared to reported and loss values recorded in 2019. Burglary recorded a reported value of approximately GH¢ 1.35 million in 2020, as compared to an approximate reported value of GH¢ 0.70 million in 2019, representing an increase of 97.7% in year-on-year terms.

## 6.0 FRAUD SUCCESS RATE

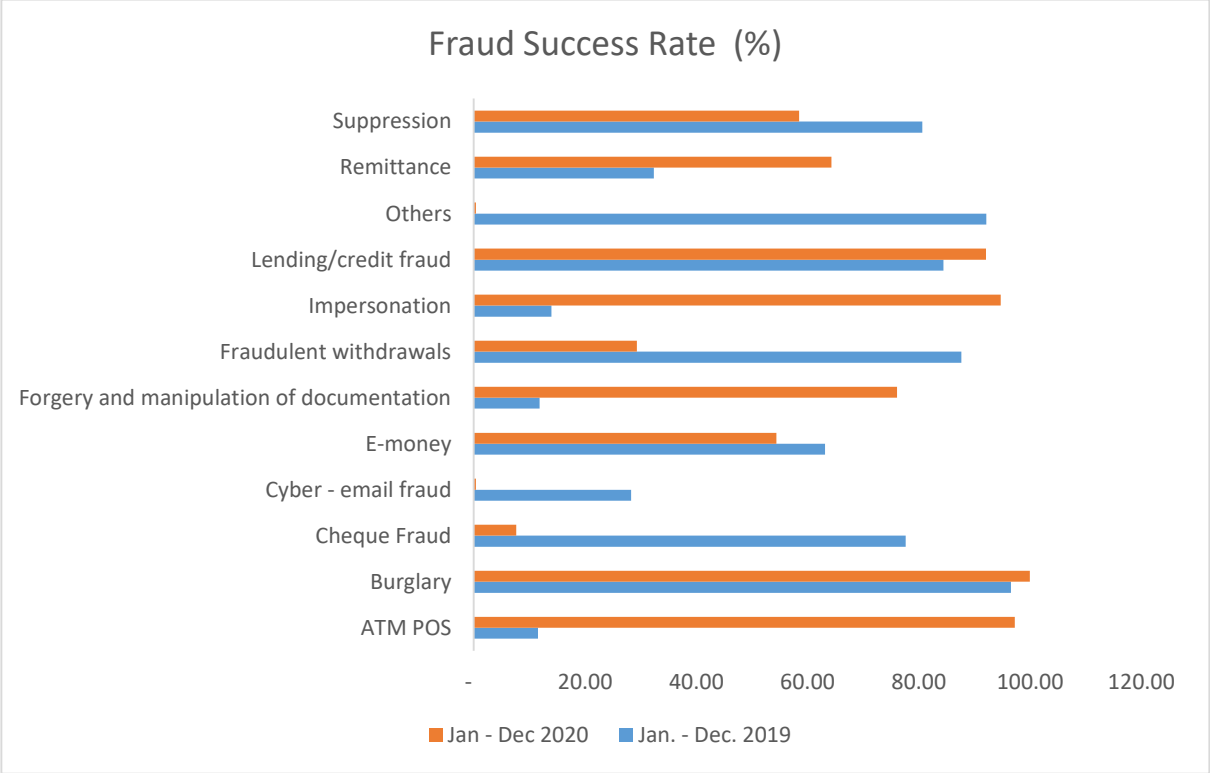
Figure 2 below on fraud success rate shows a comparative analysis of the rate of success of various fraud types that occurred in 2019 and 2020. ATM/POS fraud recorded the highest success rate of 97.3% in 2020, in comparison with a recorded success rate of 11.5% in 2019. Impersonation fraud follows closely with a recorded success rate of 94.7%, as compared to a success rate of 13.16% recorded in 2019. Remittance fraud also recorded a marked increase in the rate of success in 2020. 2020 recorded a 64.3% rate of success, as compared to a success rate of 32.4% recorded in 2019.

Forgery of documents also recorded a considerable increase in success rate for the period under review. 2020 recorded a success rate of 76.1%, as compared to a success rate of 11.8% recorded in 2019.

Some fraud types recorded notable decreases in their rate of success in 2020. Cheque Fraud recorded the most significant reduction in its success rate in 2020. The success rate of Cheque Fraud declined from 77.7% in 2019 to7.7% in 2020. The success rate of Cyber and E-mail Fraud also recorded a significant decrease from 28.3% in 2019 to 0.4% in 2020.

Generally, there has been a considerable decrease in the rate of success in the commission of fraud from 29.0 % in 2019 to 2.5% in 2020.

**Figure 2 FRAUD SUCCESS RATE**




## 7.0 SIGNIFICANT FRAUD TYPES

Data recorded for 2020 showed that different sectors of the banking industry were impacted differently by the various fraud types. Some sectors seemed more susceptible to certain types of fraud than others. Fraud types such as Suppression of Cash recorded a higher impact on sectors such as, rural and community banks

and microfinance companies. Lending and Credit Fraud recorded a higher impact on savings and loans companies. ATM/POS fraud and Cyber/E-Mail Fraud recorded a higher impact on banks.

Table 4 below shows the proportion of loss incurred from the various fraud types reported in 2020 and 2019

**TABLE 4: Loss Incurred Value per Fraud Type**

| | Loss Amount Per Fraud Type to Total Loss from Fraud (%) | |
|---|---|---|
| **Fraud Type** | Jan-Dec. 2019 | Jan-Dec. 2020 |
| **ATM POS** | 3.78 | 32.24 |
| **Burglary** | 2.05 | 5.33 |
| **Cheque Fraud** | 7.16 | 1.84 |
| **Cyber - email fraud** | 42.79 | 4.16 |
| **E-money** | 1.12 | 4.13 |
| **Forgery and manipulation of documentation** | 13.18 | 25.62 |
| **Fraudulent withdrawals** | 4.02 | 3.48 |
| **Impersonation** | 0.29 | 0.23 |
| **Lending/credit fraud** | 3.54 | 2.46 |
| **Others** | 9.77 | 10.89 |
| **Remittance** | 0.12 | 0.21 |
| **Suppression** | 12.19 | 9.42 |
| **Total** | 100.00 | 100.00 |

### 7.1 Suppression of Cash/Cheques and Deposits

Out of a total of 2,670 fraud cases reported in 2020, 1,958, representing 73.3% of total submissions were related to cash suppression. Notwithstanding this increase, the success rate of Suppression Fraud decreased considerably from 80.7% in 2019 to 58.5% in 2020. The microfinance sector and rural and community banking sector recorded the highest success rates of 68.9% and 68.2% respectively, in cash suppression fraud. This is followed by the savings and loans sector with 53.3%, the finance house sector with 44.7% and the banks with 40.9%. Figure 3 below shows the rate of success in cash suppression fraud per sector.

**Figure 3: SUCCESS RATE OF CASH SUPPRESSION PER SECTOR**

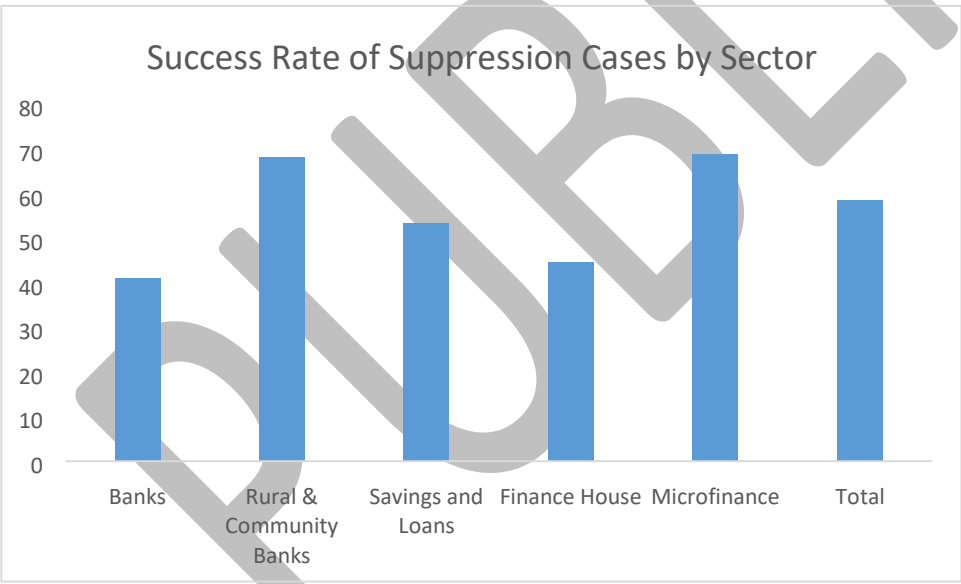
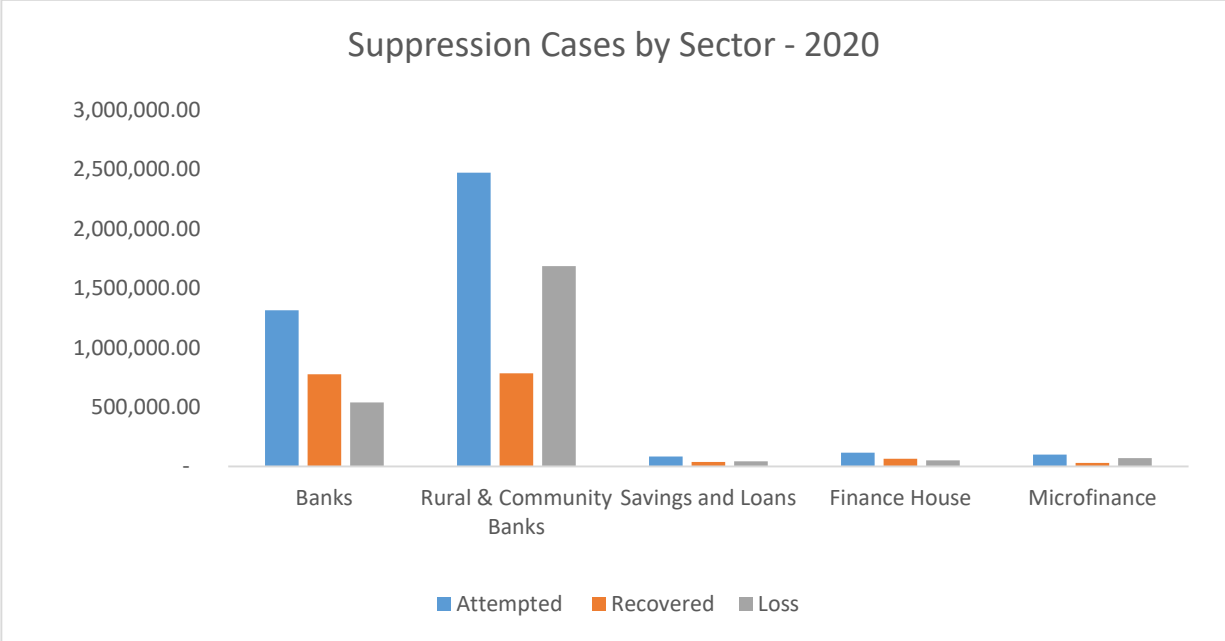



Figure 4 below shows values attempted, recovered and lost through cash suppression. Rural and community banks recorded the highest attempted and loss values. Banks and rural community banks recorded the highest cash suppression related losses in 2020. Rural community banks lost GH¢ 1,687,193.77 through cash suppression, as against a total of GH¢ 538,595.32 by banks.

Loss through cash suppression may be as a result of weak internal controls, or non-adherence of institutions in the sector, to their own security systems.

**Figure 4: GRAPHICAL DISTRIBUTION OF CASH SUPPRESSION LOSS VALUES PER SECTOR**




The percentage of staff involved in cash suppression in 2020 increased from 51.0% in 2019 to 56.0% in 2020. The heightening rate of staff involvement may be attributed to inadequate vetting processes of staff of financial institutions. Also, weak internal control systems that allow unauthorized staff to interact with customers, as well as unauthorized staff accessing confidential information and systems that should have been restricted to authorized personnel only, are the major contributory factors that lead to the escalation of this fraud type.

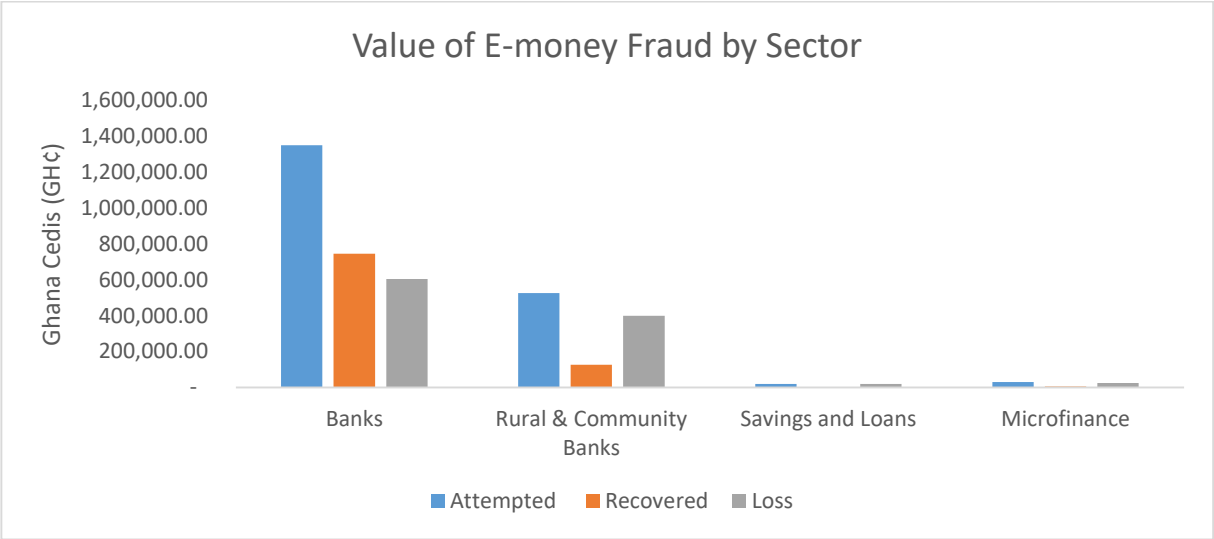
Furthermore, the inadequate levels of remuneration for temporary staff engaged by banks and SDIs as a contributory factor to the recurring phenomenon of staff involvement in cash suppression fraud, cannot be overlooked.

To mitigate the incidence of this fraud type, financial institutions especially banks and rural and community banks should undertake to reduce drastically, the engagement of contract staff in sensitive cash related positions. Banks and rural banks must also endeavour to vet their temporal staff before they engage them. The Banking sector must engage the employment agency sector to possibly set minimum remuneration standards for specific positions in the banking industry.

### 7.2 E-Money Fraud

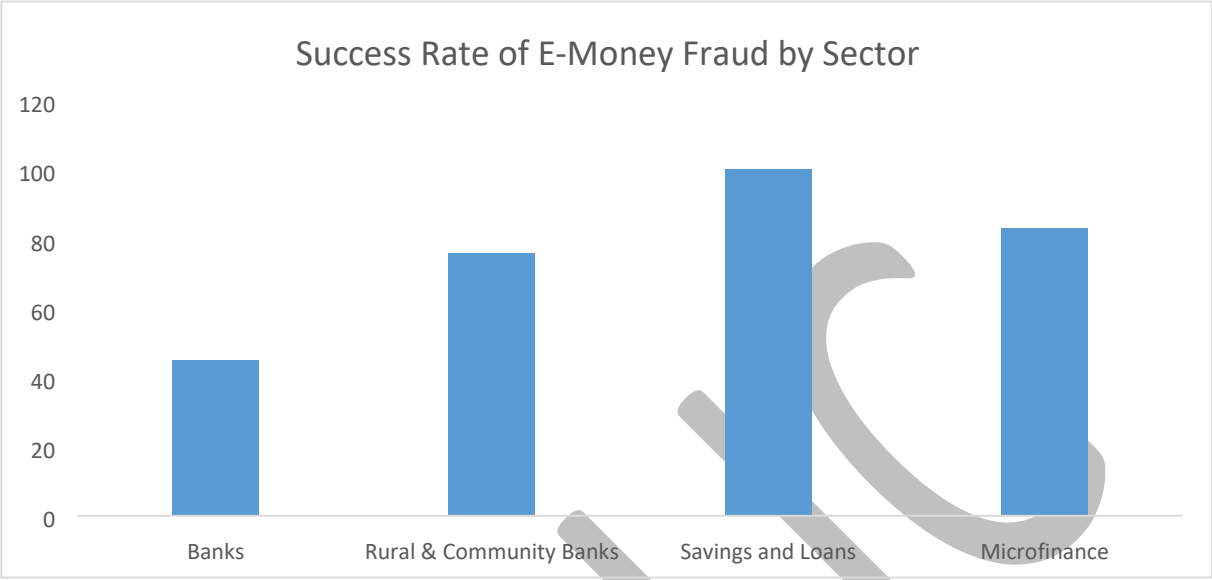
E-Money fraud recorded 14 cases in 2019 and 126 cases in 2020 showing a year-on-year increase of 800.0%. Figure 5 below show E-Money related loss values for 2020. E-Money Fraud recorded a loss value of GH¢ 1.04 million for 2020, as compared to a loss value of GH¢ 0.37 million for the same period in 2019. (refer to Table 3 above) Banks recorded the highest loss values for E-money Fraud. Banks lost GH¢604,755.65, representing 57.7% of total E-money related fraud recorded in 2020. Rural and community banks followed with a loss of GH¢ 398,883.59 representing 38.1% of total E-Money related losses reported in 2020. (refer to figure 5 below).

**Figure 5: LOSS VALUES INCURRED AS A RESULT OF E-MONEY FRAUD**




Even though Savings and loans companies recorded negligible E-Money related losses, the sector recorded a 100.0% success rate of E-Money related fraud. This may be an indication of the absence of security systems in the sector to forestall E-Money related losses. Figure 6 below shows the success rate of E-Money related fraud by sector.

**Figure 6: SUCCESS RATE OF E-MONEY PER SECTOR**




Microfinance companies follow closely with 83.09% success rate in E-Money related fraud. This is followed by rural and community banks with success rate of 75.9% and 44.8% respectively. The data indicates that sectors with less stringent security measures record higher success rate of E-Money related fraud.

Most reported losses in 2020 were related to cases of customers who were misled to transfer funds from their wallets to designated mobile money wallets whose holders are unfamiliar or unknown to the victims. On other occasions, personal identification information was compromised and subsequently used by fraudsters to transfer money from the victims' account to mobile money wallets unknown to the victims.

Another emerging trend recorded in 2020 is the impersonation of senior officials or supervisory officials in the commission of this fraud type. This new trend involves the placement of calls by fraudsters to staff in charge of e-money platforms, claiming to be a supervising manager and requesting for sensitive information that allows immediate access to e-money accounts of the affected banks, or

visiting the premises of a bank and posing as an official from its supervising institution. The imposter then proceeds to request for a demonstration of transaction reversal processes. As the staff in charge demonstrates the process on the bank's system, the imposter suggests a code to be imputed for demonstration purposes. Funds are immediately transferred from the bank's E-money account upon imputing the code suggested.

Staff of affected banks, without proper authentication of identity, give requested information to impersonators or grant such imposters unfettered access to their E-money platforms.

Other reported cases include fraudulent staff who make unauthorized transfers from the financial institution's e-money account to accounts specially created by them to perpetuate fraud.

The reported cases showed a lapse in access control and authorization systems of affected banks. These banks do not seem to have in place, systems that limit access of e-money platforms to only authorized persons. Also, they may also not have in place, levels of authorization for categorized transactions or systems that regulate staff access on their e-money platforms. There is also an obvious lack of authorization policies that prevent transactions within certain value ranges from being executed without another level of clearance from a supervisor.

The trend of reported cases also indicates a general lack of security awareness amongst staff assigned to E-Money schedules. The level of gullibility demonstrated by several of such staff who fell prey to this fraud type, indicates a lack of training on security matters relating to electronic financial transactions. Banks and rural banks should institute access control policies and authorization policies that will enable proper monitoring and authorization of transactions. Management and staff of banks and rural banks, should also implement measures to equip staff with

the requisite training that will ensure awareness of fraud related to e-money transactions.

### 7.3 ATM/Card Fraud

ATM/Card Fraud recorded for 2020 involved the fraudulent appropriation and use of customer card details for online shopping and unauthorized debits and transfers from victims' accounts through electronic banking. Other instances include incidents where culprits steal victims' cards and used them to make withdrawals from ATM machines.

Reported cases in 2020 show a general lack of security awareness amongst cardholders. Victims of such fraud usually compromise their card details or PIN details during a transaction. Their details are immediately stolen and used for unauthorized transactions. ATM/POS fraud was reported by banks only.

ATM/POS Fraud accounted for 6.3% of total fraud incidents reported in 2020, as compared to 4.8% recorded in 2019. ATM/POS Fraud accounted for 32.3% of total fraud related losses incurred in 2020, as compared to a loss of 3.8% recorded in 2019 (Refer to tables 4 and 5).

## 8.0 OTHER TYPES AND TRENDS OF FRAUD

Other fraud types such as Cyber/E-mail Fraud, Cheque Fraud and lending/Credit Fraud recorded significant decreases for the year under review.

Cyber/Email Fraud cases recorded in 2020 fell from 112 cases recorded in 2019, to 28 cases, representing a 75.0% decline in year-on-year terms. (refer to Table 2 above). Cheque Fraud recorded 16 cases, compared to 40 cases for the year under review, representing a decrease of 60.0% in year-on-year terms. (refer to Table 2 above). Lending/Credit Fraud recorded 18 cases in 2020, as compared

to 36 cases recorded in 2019, representing a decrease of 50.0% in year-on-year terms. (refer to Table 2 above).

**Table 5: PROPORTION OF FRAUD TYPE COUNT IN TOTAL FRAUD COUNT**

| | Proportion of Fraud Type in Total Fraud Count (%) | |
|---|---|---|
| **Fraud Type** | Jan-Dec 2019 | Jan-Dec. 2020 |
| **Suppression** | 76.76 | 73.33 |
| **Fraudulent Withdrawals** | 0.69 | 6.63 |
| **ATM POS** | 4.76 | 6.29 |
| **forgery and manipulation of documentation** | 6.79 | 5.66 |
| **e-money** | 0.61 | 4.72 |
| **cyber - email fraud** | 4.85 | 1.05 |
| **lending/credit fraud** | 1.56 | 0.67 |
| **Cheque Fraud** | 1.73 | 0.60 |
| **remittance** | 0.35 | 0.37 |
| **others** | 1.25 | 0.34 |
| **Burglary** | 0.30 | 0.22 |
| **Impersonation** | 0.35 | 0.11 |
| **Total** | 100.00 | 100.00 |

### 8.1 Cheque Fraud

Cheque Fraud refers to the unlawful use of cheques for the purpose of acquiring funds illegally. There are four main types of cheque fraud. They are, cheque cloning, counterfeit cheques, stolen cheques and alteration of cheques. Cheque

cloning – this refers to the use of replicas of authentic cheque leaves with identical features to illegally draw funds from and account. Counterfeit cheques – this refers to the use of non-bank paper to print cheques to look exactly like genuine cheques. These counterfeit cheques are drawn by fraudsters on genuine accounts. In some instances, the counterfeit/cloned cheque leaflets are issued and paid before the original leaflet is issued and presented for payment by the account holder. Stolen cheques – this refers to the illegal appropriation of a genuine cheque for the purpose of making unauthorised withdrawal on an account.

Recent cases of cheque fraud have seen an increase in the level of sophistry. Some fraudsters now resort to intercepting/diverting/swapping or ported calls from customers, in order to confirm payment of cloned/counterfeit cheques.

In 2020, cheque fraud accounted for 0.60 % of the total number of reported cases, as compared to 1.7% of total fraud reported in 2019. (refer to Table 5 above) Cheque fraud recorded a loss value of approximately GH¢0.47 million in 2020 representing 1.8% of total fraud related loss incurred in 2020, as compared to a loss value of GH¢2.39 million recorded in 2019, representing 7.2% of the total fraud related loss incurred in 2019. Cheque fraud recorded a percentage decrease of 80.5% in year-on-year terms. (Refer to table 4 and 5)

### 8.2 Forgery and Manipulation of Accounts and Negotiable Instruments

**Forgery** - This type of fraud involves the forgery of an authorizing signature on a genuine document, or the fraudulent alteration of a genuine document, in order to inflate the original amount. One method identified by the banking industry, is that suspects pick up balance requisition slips from dustbins in the banking hall and use the information and signature to fraudulently access funds from the customers' accounts. This fraud also includes presentation of false documents

such as educational certificates and account statements for financial consideration.

**Manipulation of Accounts and Negotiable Instruments** - This type of fraud refers to the alteration of negotiable instruments such as payment slips, payment orders, etc. and diversion of fixed deposit proceeds into private investments. These were mainly perpetrated by rural bank officials. In some cases, staff fraudulently used their profile to divert money from dormant accounts into fictitious accounts.

In 2020, Forgery and Manipulation of Accounts and Negotiable Instruments accounted for 5.7% of the total number of reported cases, as compared to a rate of 6.8% in 2019. Forgery and Manipulation of Accounts and Negotiable Instruments recorded a loss value of approximately GH₵ 6.5 million in 2020 as compared to an approximate loss value of GH₵4.4 million recorded in 2019, representing a 47.6 % increase in year on year terms. Forgery and Manipulation of Accounts and Negotiable Instruments accounted for 25.6% of fraud related losses incurred in 2020. (Refer to Tables 4, 5 and 6).

### 8.3 Cyber/E-mail Fraud

Cyber/E-mail Fraud involves the use of the internet to gain access to personal financial information for the purpose of hacking into victims' accounts and misappropriating their funds. This fraud is usually perpetuated through phishing. Phishing refers to the process of sending spam mails or forms of communication to victims with the intention of doing something that will undermine their financial security.

In 2020 cyber- related crime mainly involved e-mail fraud and fraud on internet payment platforms. Cases of e-mail fraud involved the forwarding of outward transfer instructions from the officially recognized e-mail addresses of some

customers, to their bankers. An attempt by the banking officials to authenticate such instructions led to the discovery of the fraud. Scams help fraudsters gain access to the card verification value (CVV) of victims. Fraudsters obtain the CVV of victims through phishing (i.e. the using of fake email addresses of banks to lure victims to submit sensitive data such as the CVV, or installing a web-based key logger on an online payment platform) When a key logger malware is installed, all data that the customer submits is copied and sent to the fraudster's server. As online purchases do not require the physical presence of the card being used, fraudsters are able to make purchases with the CVV. In such cases, it is difficult to determine the point of compromise. Such online payment fraud is becoming more rampant with the increase in local payment platforms.

In 2020, cyber/E-mail fraud accounted for 1.05% of the total number of fraud cases recorded. Cyber/E-mail fraud recorded a loss value of approximately GH₵1.05 million in 2020 as compared to a loss value of GH₵14.3 million recorded in 2019, representing a 92.6 % decrease in year-on-year terms. (refer to table 4, 5 and 6). This remarkable decline may be as a result of the industry's adherence to Bank of Ghana's Cyber Security Directive issued in 2018.

### 8.4 ATM / Card Fraud

ATM fraud refers to the fraudulent use of the ATM of another person's ATM card or PIN to withdraw money from an ATM machine, or stealing directly from the ATM machine. Card fraud refers to the fraudulent use of another person's card details and PIN number to make unauthorized purchases or withdraw cash from the victim's account.

ATM/Card Fraud recorded for 2020 involved the fraudulent appropriation and use of customer card details for online shopping and shopping. This mode was quite prevalent in the ATM/Card Fraud cases recorded for the period under review.

Most reported cases involved the use of the victims' card details to make purchases online, without the victims' knowledge of such transactions. Another type of ATM/Card Fraud recorded for 2020 was the unauthorized use of customers' ATM cards for withdrawals. Culprits usually stole victims' cards and used them to make withdrawals from ATM machines. This shows a general lack of security awareness of cardholders. Victims of such fraud usually compromise their card details or PIN details during a transaction. Their details are immediately stolen and used for unauthorized transactions.

In 2020, ATM/Card fraud accounted for 6.3% of the total number of reported cases as compared to a proportion of 4.7% recorded in 2019. ATM/Card fraud recorded a loss value of approximately GH¢ 8.19 million, representing 32.3% of fraud related loss incurred in 2020, as compared to an approximate loss value of GH¢1.26 million recorded in 2019, representing 3.8% of total fraud related loss incurred in 2019. Losses incurred through ATM/Card fraud recorded a 548.1% increase in year-on-year terms. (Refer to Table 4, 5 and 6

### 8.5 Impersonation

Impersonation Fraud refers to a scheme that involves an imposter fraudulently requesting for, or authorizing a payment. Some imposters may also pose as officials from the bank in order to trick victims into making payments into certain accounts. 2020 recorded a number of incidents where impersonators posed as management staff, or staff of supervisory bodies, requested and gained access to the institution's mobile money platform and made unauthorized transfers to other accounts, or issued instructions to unsuspecting staff to enable the fraudsters gain access to the institutions' mobile money platforms and make unauthorized fund transfers. Other impersonation fraud types were imposters who posed as the victims and presented ID cards bearing victims' names, in order to make withdrawals from remittance transactions.

Impersonation accounted for 0.1% of the total number of reported cases in 2020 and accounted for 0.2% of all fraud related losses incurred in 2020. Impersonation recorded a loss value of GH¢0.05 million in 2020, as compared to a loss value of GH¢0.96 million recorded in 2019, representing a 38.0 % decrease in year on year terms. (Refer to Table 4, 5 and 6)

### 8.6 Remittance Fraud

This type of fraud involves the impersonation of beneficiaries of inward remittances, especially funds sent via Western Union and MoneyGram. Incidents filed as remittance fraud involved wrong payments made as a result of fictitious identification documents presented to the banks. Unfortunately, some staff of banks in charge of processing these transactions fail to use the G-Vive platform to authenticate the identity cards provided. In other instances, fraudulent staff perpetuate the remittance fraud by themselves. After collecting IDs from beneficiaries, they deceive the beneficiary into believing that their transactions cannot be completed due to network challenges. They advise them to proceed to another branch to undertake the transaction only for the customers to realise on arriving at a different branch that the transaction has already been completed. These fraudulent staff utilize the information presented to process the transaction when they turn away the customer and appropriate their funds. In other instances, staff of banks relay personal information of beneficiaries to their accomplices, to generate fake IDs to withdraw beneficiaries' funds in other financial institutions. Remittance fraud incidents recorded in 2020 accounted for 0.37% of fraud cases reported in 2020 as compared to a rate of 0.35% recorded in 2019. Remittance fraud accounted for 0.2% of total loss incurred through fraud in 2020. (Refer to Table 3, 4 and 5)

## 8.7 Burglary

Burglary is steadily rising from obscurity and gaining ground in its impact on the banking industry. Loss incurred through burglary in 2020 accounted for 5.3% of total fraud related losses recorded in 2020, overtaking prevalent fraud types such as E-Money and Cheque Fraud in the process. (refer to Table 5) This may be as a result of laxity in the establishment and enforcement of physical security systems by some industry players, thereby exposing their premises to higher risks of invasion.

## 8.8 Others

Fraud classified as "Others" includes incidents of stealing by staff, pilferage on the premises of the financial institutions and correspondent banking fraud among others. Instances of correspondent banking fraud included situations where staff of a bank assisted a walk-in customer to procure fake SWIFT advices, in order to defraud the customer's external supplier.

In 2020, fraud categorized as "others' accounted for 0.3% of the total number of reported cases and accounted for 10.9 percent of fraud related losses incurred in 2020. Fraud categorized as "others' recorded a loss value of approximately GH₵ 2.76 million in 2020, as compared to a loss value of GH₵ 3.26 million recorded in 2019, representing a 15.4 % decrease in year-on-year terms.

## EFFORTS BY BANK OF GHANA TO REDUCE FRAUD

The Bank of Ghana collaborates with relevant stakeholders to combat fraud in the banking industry. Most of the stakeholders are members of the Committee for Co-operation between Law Enforcement Agencies and the Banking Community (COCLAB). The Fraud Task Force led by BOG, also facilitates collaboration

between industry participants and other stakeholders, with the aim of identifying the risks posed by emerging fraud trends and also developing and implementing effective controls to combat the threat of fraud to the financial sector.

Members of this committee include nominees from the telecommunication companies, National Communication Authority (NCA), Ghana Association of

Bankers (GAB) and Ghana Interbank Payment and Settlement Systems Limited (GhIPSS).

The Bank of Ghana has also made significant stride through the placement of a 24-hour monitoring system – a system known as the Cyber Incident Event Monitoring System (CEMS). CEMS monitors irregularities in transactions and log-ins in the banking sector and helps to reduce cyber fraud in the banking industry. Bank of Ghana has also issued a Cyber and Information Security Directive known as "Bank of Ghana Cyber and Information Security Directive 2018", to provide the financial sector with a framework for establishing cyber and information security protocols.

## 9.0 RECOMMENDATIONS

In keeping with its mandate of ensuring the efficient operation of the financial system and also, undertaking surveillance of the financial system to identify risks for prompt remedial action, the Bank of Ghana makes the following recommendations:

- Contract/temporary staff of financial institutions should be adequately vetted by the Police and Bank of Ghana to help identify staff with questionable characters.

- The banking industry should take a critical look at remuneration of temporary staff and, in collaboration with the recruitment industry, set equitable minimum standards of payment for temporary staff assigned to the banking sector.
- The KYC/CDD and transaction monitoring systems of financial institutions have to be strengthened in order to facilitate the detection of suspicious or abnormal activities on customers' accounts.
- E-Money issuers must enhance and sanitize their existing KYC database by acquiring authentic and verifiable bio data on all existing mobile account holders.
- Banks should provide regular and adequate consumer education on cyber security for their customers, in order to equip account holders to protect themselves from cyber fraud.
- Banks must also ensure that they activate a second level authentication in online transactions, by requesting for specific One Time Passwords (OTPs) and PINs.
- Consumers should be educated on the safe usage of digital/electronic products and services. They should also be encouraged to use efficient electronic payment methods that keep an audit trail of fund movements.

**Recommendations for the mitigation of Cyber/E-mail fraud:**

- Financial institutions and E-Money Issuers should put in place transaction monitoring systems that can identify unusual spending patterns and potential fraudulent transactions. Banks can track suspicious activities and could thus contact cardholders to check whether a suspicious transaction is genuinely theirs. If it is not, the card can immediately be hot-listed. E-Money Issuers can also use transaction monitoring systems to identify and flag suspicious activities by fraudsters who utilize their platforms to perpetuate fraud.

- The banking industry should put in place, measures designed to raise awareness of cyber/e-mail related crime among consumers.
- Information sharing between banks on counter-measures against fraudulent activities should be encouraged to help protect the industry and its customers from fraud. This could be achieved by the use of a Fraud Intelligence Sharing System (FISS) which offers the benefit of sector-wide intelligence. Members could exchange a range of information on the FISS platform. The FISS is a central industry database – an extremely secure, flexible and cost-effective intelligence system designed to support the card and retail banking industries in the fight against fraud. It can be used to identify linkages and patterns in frauds, thereby playing an important role in protecting consumers.