"THE CURRENT SPATE OF FINANCIAL CRIMES WITHIN BANKS IS A SETTING A VERY DANGEROUS PRECEDENT"

There is an adage that "crime follows opportunity" and since banks deal in lucrative financial products, they will continue to be targeted by criminals either from within or without to perpetuate financial crimes. With the spate of recent Bank frauds, the regulatory focus including in banks should be more on employees than on the customer of the bank. The Uganda Bankers Association (UBA) website offers information how to safeguard against on financial crimes threats. Banks have also adopted internal measures such as Know Your Customer (aka KYC) to safeguard against financial crimes. However, it needs to be noted that no single safeguard measure is a silver bullet. Most recently companies have used artificial intelligence (AI) to enhance their capabilities in real-time fraud-detection improvements and to provide instant solutions. The FATF has, for instance, suggested that in some circumstances banks may start to use robots to automate certain activities such as populating case files for investigators, the closing of level one alerts, and population of suspicious activity reports (SARS). Since the robots work is directed by a human mind, it cannot change a lot without first changing the human mind-set.

The practice when banks suspect a debit or credit card fraud has been to talk to the individual cardholder as soon as possible. Speed is of the essence to communicate with the cardholder and to solve the problem as soon as possible. The faster a customer can talk to the bank, and the faster the bank can engage with the customer, the faster genuine fraud can be mitigated, minimising financial losses on both parties. Speed has an additional positive impact on the relationship between the bank and the cardholder by reducing friction in the transaction process, minimising customer frustration against the bank. Communication with the cardholder has proved to be the most powerful tool in the bank's arsenal to fight fraud. Some banks have connected card issuers and users to share fraud information in near real-time to ensure intelligence is used effectively. Fair Insurance Corporation (FICO), recently reported that credit card fraud in Europe has risen from 50 percent in 2008 to 70 percent in 2016. This same report estimates that 72 percent of card losses are suffered by issuers and banks have collectively injected billions of money into protecting their customers and their reputations.

Banks need to check customer's profiles

Banks are required to check customers' contact details at every interaction point: online, over the phone or face-to-face at a branch. Banks need to make sure customers email addresses are up-to-date and still used; check that you have their personal cell numbers; and find out how to reach them at work. If the bank does not have the right contact details about the customer, investigations about the customer cannot be undertaken. If a bank blocks a good transaction (called a "false decline"), it risks frustrating its customers and losing their loyalty. The cardholder often elects to put the card at the back of the wallet, where it tends to stay—either permanently or for some time before it is used again. Research indicates that 475 million cardholders globally are at risk of relegating a preferred card to the back of the wallet after it has been declined by a bank. Using advanced collaboration techniques, banks are not only endowed with the potential to provide cardholders with details on the date, time and cost of the purchase, but also with information about the retailer and even the specific product/service that was purchased. Banks must exchange information with the customer to

make a quick decision based on the bank's detailed description of the transaction. It would also be helpful for banks to recruit and work with credit card fraudster, if they can identify them even if it might not necessarily be the best approach, if it gives them results to stamp out fraud. By recruiting customers, banks can establish a powerful, cost-effective tool and a network against fraud, money laundering and other financial crimes to make it safer for both the bank and customers. Banks will however also need to enact measures that to protect against employees who use their positions to perpetuate fraud against the banks and its shareholders.

Banks need to operate with integrity

In early 2000, due to introduced changes as a result of heightened terrorist threats, many international Banks were criticised in the way they handled suspected money laundering cases. Upon forming suspicion of financial fraud and for fear of tipping off a customer, Banks would act in haste to freeze customers' accounts without giving them the reasons for doing so. In the aftermath. A study was conducted by the Guardian Newspaper (UK) in 2010, it found that 80 percent of Banks do not educate consumers on how to safeguard against financial such as credit and debit card fraud. Banks will need to innovate ways and means on educating customers about potential vulnerabilities in using credit and debit cards and measures to adopt in safeguarding from potential fraud. This should include communication with simple with customers in a language free terminology and technical jargons to sensitize them against fraud. One time I visited an ATM in Mbarara in get some money, when I entered the booth there was this lady who seemed not to know how to withdraw money from her Account and was asking for help—which was to say the very least very unprecedented. The issue here was that this bank customer seemed not have been sensitised on the dangers of someone using her card to perpetuate a fraud against her. I therefore propose the public/private partnerships in regulatory oversight of Banks. Bank supervision is a practice carried through a number of mutually self-supporting processes, generally based on regular returns, meetings, regular or *adhoc* visits, reports and investigations in individual banks." It uses internal measures such as checking the robustness of Know Your Customer (KYC), Suspicious Activity Reports (SARs)/ Suspicious Transaction Reports (STRs), Customer Due diligence (CDD), Enhanced Customer Due Diligence (ECDD) and others. This will bring in an element of public-private partnership in providing effective oversight and protection of shareholders equity. Both the bank and the private sector have a stake in the way financial institutions are regulated. The Government is the guardian of these interests for members of the public since it will come in to pick the pieces when things go wrong.

In a situation where regulatory safeguards within banks are compromised by employees, treating shareholders equity as personal property, using banks assets as they please in total disregard of prescribed regulatory guidelines, sets a dangerous precedent. There must be a clear divide bank employee cannot afford to cross—to know that ultimately the truth will bubble to the surface.