TEMENOS
THE BANKING SOFTWARE COMPANY

NetGuardians

A-Z of Financial Crime in Africa

The What, Why and How to Tackling Financial Crime in Africa

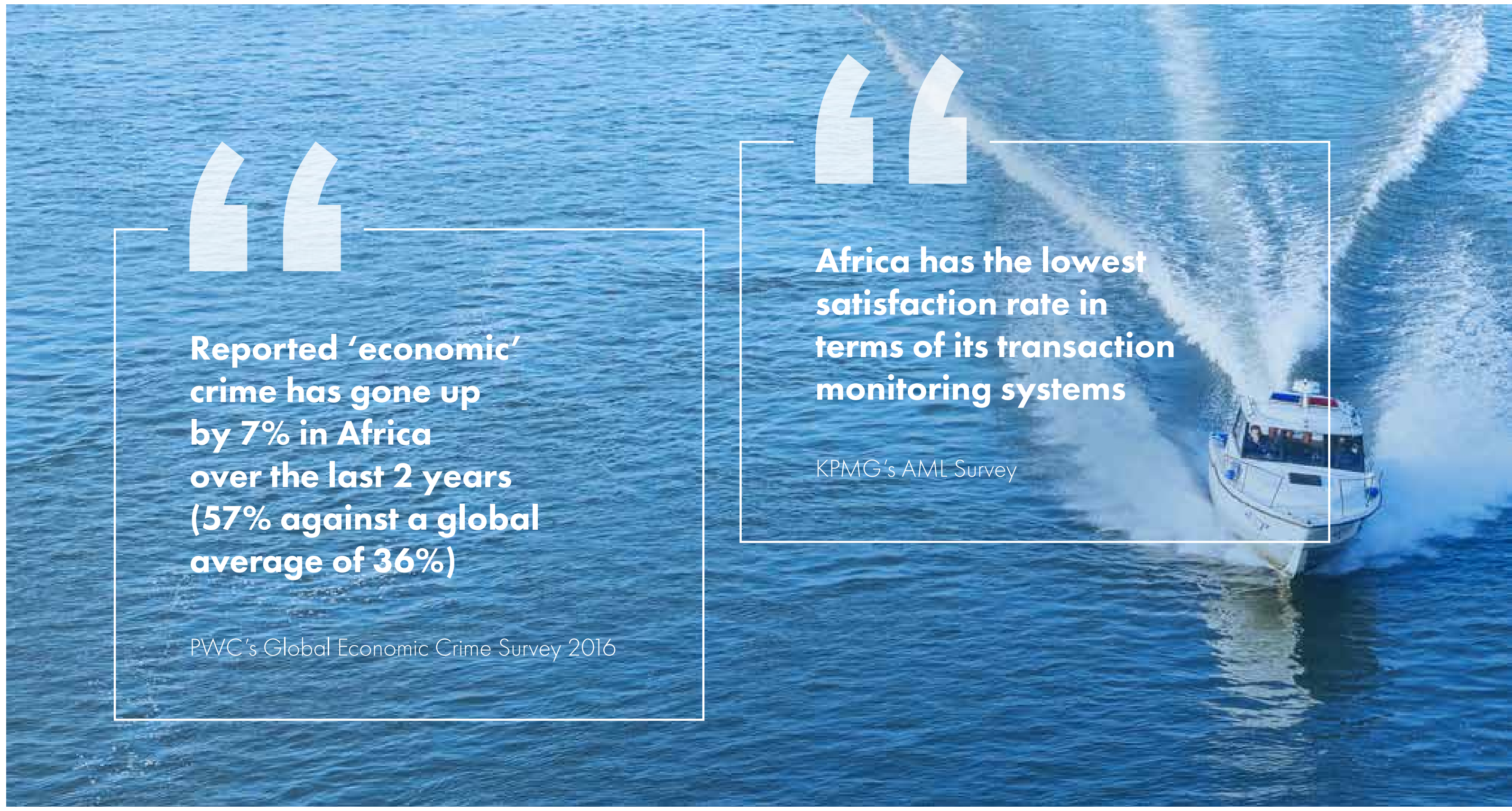
Contents

Introduction

Perhaps nowhere are financial crimes, including fraud, more serious and more pronounced than in the banking sector of the economy. They are one of the biggest single causes of bank failure and distress in the African banking system. In general, Africa is the most vulnerable and currently the most affected by financial crime in comparison to any other continent. According to PWC's Global Economic Crime Survey 2016, reported 'economic' crime has gone up by 7% in Africa over the last 2 years (to 57% against a global average of 36%). And KPMG's AML survey[1] listed Africa as having the lowest satisfaction rate in terms of its transaction monitoring system. There has therefore never been a more important time to have a full understanding of this issue and review existing systems to ensure the areas most open to abuse are addressed.

Welcome to the Temenos and NetGuardians **A-Z of Financial Crime in Africa**. A comprehensive e-book outlining the what, why and how of financial crime within the fastest growing continent. Temenos and NetGuardians have teamed up to compile this indispensable A-Z guide exploring the size of the issue, who commits it and, most importantly, what can be done to mitigate against it. We hope it's thought-provoking, not too worrying, stimulates discussion, and provides guidance and reassurance for the future.

Yours truly,
Amanda Gilmour, Financial Crime Product Director, Temenos
Joel Winteregg, CEO, NetGuardians



> **Reported 'economic' crime has gone up by 7% in Africa over the last 2 years (57% against a global average of 36%)**
>
> PWC's Global Economic Crime Survey 2016

> **Africa has the lowest satisfaction rate in terms of its transaction monitoring systems**
>
> KPMG's AML Survey

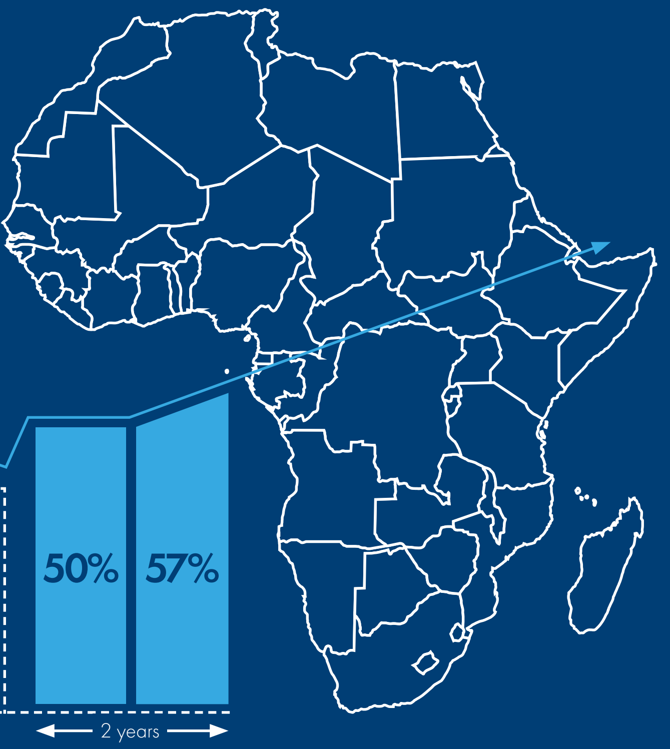
[1] KPMG Global Anti-Money Laundering Survey (2014)

Quantum of Financial Crime in Africa

The scale of financial crime committed in Africa is hard to determine in part because many cases go unreported. However, information from within the industry (and on economic crime in general) suggests that:

67bn
Total value of banking fraud in 2014[2]

3-5%
of global GDP is estimated to be laundered worldwide on an annual basis[3]



Africa as a region experienced the **largest increase in economic crime** since 2014.[4] Economic crime has increased from 50% to 57% in Africa in 2 years.[5]

6%
of banks' global pre-tax profits were lost as a result of criminal activity[6]

92%
of financial institutions within the region state that money laundering is high risk[7]

141%
increase in the number of financial firms globally reporting losses of between **$10m** and **$19.9m**[8]

[2] Association of Certified Fraud Examiners
[3] International Monetary Fund 2014
[4] Global Economic Crime Survey by PricewaterhouseCoopers (PwC), interviewing 6,337 participants across 115 countries, most of them upper level executives: 45 per cent were C suite executives (chiefs), while 30 per cent were heads of departments or business units.
[5] Global Economic Crime Survey by PricewaterhouseCoopers (PwC)
[6] Value of banking fraud calculated as a percentage of total pre-tax profits of top 1,000 banks in 2014, according to data from The Banker
[7] KPMG Global Anti-Money Laundering Survey 2014 (Respondents came from a wide range of AML-related professional backgrounds across the financial services industry.
[8] 2014 US State of Cybercrime Survey

Analytics

In modern banking, where huge numbers of standardised transactions are automated through straight-through processing, the need to implement and enforce a well-structured set of controls is paramount. These automated controls constitute the first line of the bank's technology-based defences against attempts to carry out fraudulent transactions, because they define the parameters of legitimate activity.

However, in order to ensure that the automated controls built into the bank's IT systems are operating effectively and are not being over-ridden or bypassed, they must be constantly monitored. Transaction analytics is the process of carrying out this monitoring so that any breaches of the bank's system of controls will result in security alerts being raised. This enables appropriate action to be taken. Therefore, using transaction analytics enables a bank to automate part of its internal audit process and ensure that it is applied continuously and effectively.

Transaction analytics offer a major advantage over traditional methods of checking internal controls, in that it can be applied to every transaction that the system processes. Previously, manual sampling was used to check that controls were being applied properly, with the results of the sample being used to draw conclusions about the system overall.

However, not only is manual sampling labour-intensive, slow and expensive, it also leaves the majority of transac-tions untouched. By automating the process of analysing transactions to detect breaches of controls, banks can achieve a much greater level of scrutiny than traditional methods allow.

The Financial Crime Analytics Opportunity

Predictive analytics of big data offers huge opportunities for retail banks. But historically big data adoption within the region has lagged behind the global trend in adopting this opportunity. Studies have shown that banks that effectively use Big Data to focus customer analytics show a 4% gain in market share over competitors. However, an IBM report focusing on Nigeria and Kenya revealed that 40% of businesses are in the planning stages of a big data project, in comparison with the global average of 51%. And while many large corporates in South Africa, as well as Africa, have the infrastructure in place to handle Big Data, a survey by Strategy Worx shows that many of these organisations do not use big data and analytics in any significant manner. According to a survey by Microsoft and Celent in 2013, only 37% of financial banks internationally have practical experience in using Big Data. This number is considerably lower when one considers banks in emerging economies along with many traditional banks adopting silo approaches instead of pooling data from the entire organisation. Anti-money laundering software offers this complete picture. It should hold all the transactional information on the customer in one record, regardless of how many accounts they have (credit card, current account, savings, etc.). And this transactional information often provides a picture of several days, providing a detailed insight of the customers' recent behaviour. With this information on the payments and spending patterns of customers, banks can start to direct very targeted offers to their customers.

Banks already realise the benefit of peer grouping and segmentation; this information is held in financial crime mitigation software. This presents a significant opportunity to measure and understand trends. For example, highlighting a large debit from a savings account, coupled with a smaller transaction with a furniture removal company and an interior shop, may offer the opportunity for the FI to cross-sell home insurance. The opportunities are endless when you combine information from several account sources, but with many banks having disparate systems that struggle to talk to each other, the FCM system provides the only holistic view. It is the cleanest unified set of data in a bank.

The benefit of big data from a corporate banking perspective is also strong.Using data to drive value-added customer insights and getting that information to corporate treasurers at the time and place they need it, over their preferred channel, offers huge opportunities to corporates in their trade and cash management activities. However, 30% of respondents in the IBM survey said they were unsure about whether big data projects had security benefits and 22% claimed that they did not.

Bitcoin and Blockchain

African banks have been late to embrace FinTech. However, after huge swaths of the region's population now use telcos for their financial services (most famously Safaricom's M-Pesa in Kenya), we are increasingly seeing the continent as a testing ground for new financial technologies like bitcoin and the blockchain. However, what risks (and opportunities) should be considered from a financial crime perspective?

Bitcoin

Cryptocurrencies or virtual currencies such as Bitcoin (which tends to have the most focus as it's the most well-known) have recently been at the centre of sensational headlines involving money launderers, illegal weapons sellers, drug dealers and criminal hackers etc. across the globe and Africa is no exception. This type of currency has particular appeal to criminals mainly because it offers criminals a greater level of anonymity than existing electronic payment systems. The ability to purchase the currencies with cash, the ease of moving digital funds across borders, and the lack of restrictions on deposits and withdrawals makes it particularly appealing. Concern around this technology was reinforced at the end of last year, when the Central Bank of Kenya (CBK) issued a cautionary statement similar to those of other banks in previous years citing alleged security concerns.

The decentralised structure of cryptocurrencies and the way that data can be hidden means that prosecution authorities are unable to block or seize assets. In addition, secrecy can be enhanced by anonymising tools, mixer or tumbler services that scramble transactions making them harder to trace. Other methods criminals benefiting from cryptocurrencies use, is by having multiple accounts per user and dark wallets that offer extra concealment for virtual currency users. Transacting in cryptocurrencies also requires a low level of information at present. Transactions are sent to a public network for verification. Although both parties' cryptocurrencies and Internet Protocol, or IP, addresses are transmitted to the public network, no additional information is provided about either user. However, since Bitcoin transactions for example are digitally recorded, authorities should still be able to discover who has made a transfer. But it currently requires considerable effort to do so. To address this cryptocurrency transactions need to be brought within the scope of anti-money laundering law; subject to record-keeping and verification procedures as well as the obligation to report suspicious transactions.

But the risk cryptocurrencies presents isn't just from a money laundering perspective. There have been a number of security incidents in which cryptocurrencies wallets or other infrastructures have been compromised. These incidents have exposed users to either theft of Bitcoins for example or theft of personal information given to Bitcoin exchanges.

Blockchain

The potential for blockchain to help understand global transactions in real-time could prove to be invaluable for regulators as well as financial institutions. The way that the distributed ledger technology works means institutions would potentially be able to address regulatory requirements around financial crime, such as Know Your Customer (KYC), Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT).

Transaction Transparency

Blockchain offers a financial transaction ledger that is extremely difficult to break or fool, providing details on everything that took place relative to a transaction or series of transactions, until your computer hard drive holding the ledger ran out of space. And with the block-chain, everyone over a large number of computers has the same ledger, so no single person could fraudulently modify it without everyone else immediately knowing. This also means computers could sit and monitor the blockchain for suspicious activity without needing to know any per-sonally identifiable information. And it's fast enough that it could perhaps provide an accurate chain of events across multiple trusted institutions. It can catch in microseconds if something funny, like uncharacteristic account activity, raises suspicions.

Taking a cryptographic "fingerprint" of a transaction and adding it to a ledger that everyone across the enterprise has is both accurate and virtually impossible to hack. Once you create a transaction fingerprint for every transac-tion that takes place across the whole enterprise, everyone gets a copy automatically of the updated crypto-ledger. Any future transaction associated with the same money would reference the last fingerprint, and so on, forming a really strong chain of events. In summary, knowing a whole history of transactions with a very high degree of certainty invariably increases the changes of a financial criminal being caught.

Reducing Paperwork, Reduces Risk

In addition, blockchain could drastically reduce fraud and simplify all the paper documentation from invoices through to warehouse receipts and letters of credit. This is because it introduces transparency at every stage of the supply chain by revealing the provenance of each component to everyone involved.
There is also scope for the technology to be deployed by banks to secure and meet regulatory requirements on KYC and AML registries and surveillance. And if processing times move to near real-time, more accurate feedback on risks and exposures would be available, reducing counter-party risk.

Central Data Store, Offers Greater Clarity

For financial institutions that operate across multiple entities and jurisdictions, blockchain's ability to provide a centralized store of data or information offers particular appeal as a single view of each client can easily be created. In addition, blockchain could avoid the fragmen-tation and duplication of due diligence data by recording customer data centrally, and then making this record available across the entire organization.

Blockchain in Africa

The opportunity that this technology offers the region was recently highlighted in a limited survey[9]. In conclusion the respondents from this survey are clearly leaning towards Blockchain technology providing opportunity in disrupting businesses and offering new growth for startups across the region.

There is plenty happening in Africa with bitcoin, blockchain, digital identity and digital currencies to transform the continent from one where moving money is slow, expensive and often open to fraud to one that is fast, free and trusted. However, distributed ledger technologies are so new, so complex, and evolving so rapidly that it's difficult to predict what form they will ultimately take or even to be sure they will work. There are working/discussion groups and labs that are available for banks to explore and develop technology to support their needs. In the meantime, until blockchain technology matures and the regulatory environment advances, the best option for market participants is to upgrade existing legacy systems and automate manual KYC processes.

[9] BitHub.Africa community survey February 2016

Complexity and Customer Due Dilligence CDD

The African banking market is rapidly growing, both in client numbers, as well as in the number of channels that banks use to interact with these clients. Complexity represents probably the most important source of vulnerability that African banks suffer in attempting to detect and prevent fraud. In general banking has become increasingly dependent on technology, and in the absence of a countervailing strategy, the systems that banks depend on to deliver their services have multiplied and grown much more complex. The effect of this process of increasing complexity has been to create more opportunities for financial criminals to gain access to critical systems, while at the same time making it harder for banks to have a clear overview of all the activity taking place on their systems.

Complexity in bank systems can be seen in the growing number of channels through which banks now deliver their services, including websites and online banking platforms, mobile banking services (eight of the ten countries that make the most use of mobile financial services live in Africa) and social networks. All these channels represent a new set of opportunities for fraudsters to gain access to the bank's information system. Banks' IT has become more complex as new information systems are implemented on top of older systems, building up layers of technology that do not necessarily link together and so make it much more difficult to gain a unified view of operations. As mainframes have given way to network computing, critical systems have also become more distributed: today even a relatively small institution will have multiple databases running on different servers that are accessible to a large number of staff. Complex and highly distributed IT systems such as these are difficult to police and present more opportunities for fraudsters to gain entry. Modernising the legacy systems on which many banks still depend can also increase their ability to detect financial crime, a factor that is often overlooked.

Cutting Through the Complexity

The right software should be able to effectively screen a customer database, payments and any other type of transaction, and compare these against sanctions lists, whilst following the 'four eyes' rule as a minimum default for both possible incidents of money laundering and sanctions. Even if a master customer record has been created to address these possible issues, without the right software to update this information, it may quickly become outdated. And software should also be sufficiently intelligent to identify when a transaction is matched up legitimately, yet there isn't a sanction applied or an incident of money laundering. This is often referred to as a 'false positive' (see **W is for Wrong Person**).

From a regulatory and compliance perspective, many African governments are also looking to banks to reduce complexity by transforming the way that money flows through the economy more broadly. Utilising mobile banking and payments capabilities can help to reduce the reliance on physical cash and improve anti-money laundering (AML) and risk management overall.

Customer Due Dilligence CDD

Enhanced due diligence (EDD) is a more detailed standard than know your customer (see **K is for Know Your Customer (KYC)**) required for larger customers and transactions before a new customer is on-boarded. In some countries, laws dictate that institutions establish appropriate, specific, and, where necessary, enhanced, due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering through those accounts. In addition, they often require that EDD measures are applied to account types such as Private banking, Correspondent account, and Offshore banking institutions. Because regulatory definitions are neither globally consistent nor prescriptive, financial institutions are at risk of being held to differing standards dependent upon their jurisdiction and regulatory environment. EDD should follow a rigorous and robust process of investiga-tion over and above (KYC) procedures, that seeks with reasonable assurance to verify and validate the customer's identity; understand and test the customer's profile, business and account activity; identify relevant adverse information and risk; assess the potential for money laundering and/or terrorist financing to support actionable decisions to mitigate against financial, regulatory and reputational risk and ensure regulatory compliance.

Once on-boarded, regular reviews help keeping up to date with changes during the whole lifecycle of a customer relationship that a bank maintains. Whilst linked analysis supports a bank to better understand all the connections and hidden links a customer might have with his business partners, family members, legal arrangements or even with employees, negative media research allows staying alert in case a customer's reputation derogates over time. Also knowing about potential private connections with employees could help to prevent internal fraud.

The African financial sector is increasingly embracing technological aids, in particular, biometric applications to assist in ensuring effective and accurate due diligence processes. Identification and authentication are two conceptual terms in relation to Know Your Customer (KYC) due diligence processes that have proven to be the one of the most challenging compliance functions both in Africa and internationally. Within this context, biometric applications are proving to be extremely helpful in establishing the accurate identity of customers. However, certain challenges exist with both the implementation of such biometric systems and its associated vulnerabilities in terms of technological efficiency and the various methods in which such systems can be manipulated. It thus becomes imperative for financial institutions to first research the various types of biometric systems in terms of technological efficiency and criminogenic risks. This will help facilitate quicker and easier facilitation of such systems into institutions in terms of customer acceptance, staff education and of equal importance, limited risk of manipulation of such systems[10].

[10] Anti-Money Laundering Journal of Africa, 2016, Volume 2, Issue 2

Data

Issues With Data

Your financial crime system is only as good as the information it uses. The wide variety of financial crime techniques are ever-increasing. To counteract this, decades of records, external data sources and true cases must be collated and referred to, to facilitate the identification of possible money laundering activities or sanctions breaches. It is therefore essential that this data is accessible, either through the bank's own systems or a third-party provider.

A common issue with AML and sanctions screening is that a system needs to allow for irregularities. In many cases, an FI's data will contain gaps and inconsistencies. This may have come from established clients whose data was not fully captured, regularly updated, relevant data spread across disparate systems, or simply the inability to capture some types of information. However, the right software should be able to effectively screen the customer database, payments and any other type of transaction, and compare these against sanctions lists, while following the 'four eyes' rule for alert review as a default for both possible incidents of money laundering and sanctions breaches. Even if a master customer record has been created to address these possible issues, without the right software to update this information, it may quickly become outdated.

But the issues don't always lie with the FIs' data. There are often issues associated with the sanctions lists that the data is matched against. They may be poorly structured, or have incomplete or inconsistent records, and there is a risk that bad data is being matched to bad data. One method of addressing this is to use a system that contains wizards to test newly-published public or private lists, highlight areas for improvement, enrich data with additional variations and permutations, and apply rules to avoid false detections. There is also the issue of coping with the increasing number of official lists to check against and their different formats.

Data Theft

Although most people might think of fraud as the act of carrying out illicit transactions, data theft plays a very important role in facilitating the crime and is an area of great concern for banks and their regulators. Banks hold very large quantities of sensitive data on their customers and confidentiality is a basic expectation of any bank cus-tomer. Theft of confidential data is therefore damaging to a bank's reputation, even if there is no direct financial loss as a consequence. And with a recent survey by Citrix demonstrating that half of South African workers would feel more violated if files were stolen from their computer than if intruders broke into their home, the importance of securely holding bank data has never been more important.

Data thefts can occur as a result of outsiders gaining access to information systems, but are just as likely to result from internal breaches carried out by staff with high levels of access, such as database and systems administra-tors. There is a thriving black market on the internet in stolen customer information, including online bank and credit card details.

In the most famous example of a large data theft, computer specialist Herve Falciani stole the details of 24,000 private banking clients from a branch in Geneva while working on an IT project in 2007. He subsequently passed the stolen files to French tax authorities. In this instance, the data theft did not facilitate fraud against the bank or its customers, although it did produce a strong response from the bank's regulators because of the serious breach of client confidentiality that resulted. In recent years financial regulators have stepped up pressure on banks to improve their controls around data security and to provide greater protection of clients' confidentiality. The Swiss regulator, FINMA, has published new rules on the security of client identifying data.

A more recent example was when $13 million was stolen from ATMs in Japan using stolen South African bank data. According to reports, coordinated fraudsters hit ATMs at 1,400 Japanese 7-Eleven stores in May 2016. In less than three hours, a coordinated group of fraudsters stole 1.4 billion yen (about $12.8 million), by simply strolling into 7-Eleven and withdrawing those stacks of cash from the ATM. The fraudsters reportedly used fake credit cards that were created using stolen data on roughly 1,600 account holders from Standard Bank in South Africa. Police be-lieve over 100 money mules might have been involved in the withdrawals, which took place the morning of May 15. Approximately 14,000 withdrawals were made -- each the maximum amount of 100,000 yen (~$913 US) -- from about 1,400 machines in Tokyo and 16 prefectures in Japan. 7-Eleven stores were hit presumably because they accept foreign credit cards, while many ATMs do not[11].

US$13m
stolen from ATMs in Japan using
stolen South African bank data

[11] http://www.darkreading.com/attacks-breaches/$13-million-stolen-from-japan-atms-via-stolen-s-african-bank-data/d/d-id/1325627

External Fraud

External fraud, in which an outsider manages to penetrate the bank's data security and access sensitive information or carry out fraudulent transactions, can be achieved in a variety of ways. Poor password security, for example, might allow a fraudster to gain access to the bank's information systems without the need for sophisticated computer hacking. So how does fraud compare across the continent?[12]

External Fraud in South Africa

Along with Nigeria, South Africa has one of the highest number of reported fraud cases on the African continent, and due to the size of its economy more fraud cases are to be expected[13]. A vigilant media, particularly in South Africa, contributes to the reporting of fraud and corruption cases.

External Fraud in Zimbabwe

In Zimbabwe, fraud has been increasing especially after the dollarisation of the economy. With the dollarisation, the basic economic fundamentals started to apply, resulting in significantly reduced income streams for certain classes of the society who were engaged mainly in the informal sector where returns were significant. Those with reduced sources of income tend to resort to fraudulent activities to sustain their lifestyles. In addition, according to KPMG, there are more fraudulent transactions involving individuals within the country, though the ones where companies are affected tend to be of significantly higher values. However, it is felt that the government is not directly addressing fraud as there is no known targeted response. However, businesses and banks are stepping up awareness of fraud and fraud prevention through workshops. Frauds are normally reported on as the media has a huge appetite to report on them openly.

External Fraud in East Africa

In the East African region, Kenya in standing out with 7.75% of reported fraud cases, well ahead of Uganda (2.98%) and Tanzania (2.78%). Most fraud in Kenya targets government and financial sectors as elsewhere on the continent. "Fraud and misappropriation is high, as is bribery and corruption. But we believe that a lot of cases are never reported," says William Oelofse, KPMG's East Africa Director responsible for Forensic Services. "People are reluctant to report fraud since they do not have faith in the system from a prosecution and conviction perspective and do not want to jeopardize their businesses and brands. But there is a lot more reporting than in the past."

Kenya has recently become more serious about fraud prevention. The conviction of former Tourism permanent secretary and Kenya Tourism Board (KTB) ex-managing director was hailed as a major success. Both government officials were convicted of conspiracy to defraud the ministry of Sh8.4 million (about US$100,000). They received heavy jail sentences and fines for misappropriating public funds.

In terms of other countries in the region, fraud cases in Uganda and Tanzania should also be high but it is possible that people do not seem to be comfortable reporting cases. However, in Rwanda fraud has dropped to an all-time low in recent years.

External Fraud in West Africa

Nigeria experiences high levels of fraud and corruption, a legacy stemming from the military era which lasted until the elections in 1999. There have been a lot of cases involving the banking and the oil and gas sectors or government that lead to prosecution. The current noticeable trend is that many cases either end with a plea bargain or are simply closed without any conviction. The general belief in Nigeria is that the legal system is not effective enough. In the West African region, oil was recently discovered in Ghana, nurturing a sense that the level of fraud and corruption issues from Nigeria may be replicated there.

External Fraud Supported Internally

Mobile banking is the channel of choice for the majority of Africans. Mobile phones are now an accepted way for banks to authenticate a user's identity without them being present. This opens up a new potential vulnerability in the bank's controls that can easily be exploited by an external fraudster colluding with a bank employee who has access to the bank's customer relationship management database. In order to carry out the fraud, the employee temporarily changes a customer's mobile phone number on the bank's database to the number the fraudster will use. The external accomplice then calls the bank's helpline and resets the customer's account password, using the mobile number now showing on the bank's database to validate his or her identity. Once the account has been raided, the bank employee changes the mobile number shown on the database back to the correct one and the fraud is complete. This demonstrates how easily a database administrator can make changes to a customer's information without creating an alert suggesting that controls have been breached. However, much of the fraud carried out by outsiders in fact depends on help and collusion from employees, who may have been paid relatively small sums of money to facilitate the crime.

[12] KPMG: Barometer assesses fraud risk when investing in Africa 2012
[13] The same can be observed in Nigeria and Kenya.

Four Eyes

Applying the four eyes principle (as well as the maker-checker principle) is essential to accurately identifying if a transaction is actually associated with financial crime. However, this approach can be open to abuse as we will discuss.

The four eyes principle is usually the default method of validating a huge range of day-to-day procedures carried out within a bank. This simply means that operations carried out by one member of staff have to be validated by a second person to ensure they are in line with the bank's internal controls. In the majority of cases, this segregation of duties provides a simple way of ensuring that the bank's controls are effective and that rogue employees are not able easily to circumvent them.

However, the four eyes principle is clearly vulnerable to collusion between two or more employees who by acting together would be able to break down the normal segregation of duties and validate fraudulent transactions without raising any suspicions within the bank. Because frauds of this sort take place within the bank's existing system of controls they remain under the radar and are therefore extremely difficult to detect. Collusion between staff members therefore remains the easiest way to commit fraud within a bank.

Aside from direct collusion, employees may also be able to defeat the four eyes principle if there is poor password security within the bank. If a staff member is able to gain access to a colleague's passwords, he or she may be able to carry out fraudulent operations on the system and sign in under another person's identity to validate them. As before, frauds carried out in this way are likely to be very difficult to detect among the larger number of bona-fide transactions that the bank processes every day. Besides this, the four eyes principle may be compromised if the reviewer or checker clicks through the control items without actually reviewing them thoroughly, assuming that the items are OK like they used to be in the past or because the maker would have done his job scrupulously.

In addition, some compensating controls can be applied to help detect collusion e.g. same transaction where the maker and checker was done from same IP; transactions done by users on leave or transactions done by users who are currently not in the branch by correlating transactions with access control systems etc.

Global

Financial crime can often span more than one jurisdiction and therefore a global consideration must often be made. This is particularly the case where it involves multinational organisations such as large banks that have operations in numerous countries. Global consideration may also apply where elements of the crime are directed from or carried out in another part of the world or with reference to sanctioned entities or to money laundering activities. From a fraud perspective, where the transaction has been carried out using digital information systems, it is possible that the activity may technically have taken place in more than one jurisdiction and so different countries' legal authorities could become involved.

In practice, legal authorities have demonstrated in recent cases that they are prepared to claim jurisdiction over activities that involved perpetrators operating from other territories, especially where these crimes involved global financial markets. The fines imposed on US and European banks in May 2015 for their roles in attempting to rig foreign exchange markets are a case in point. The US Department of Justice and the UK's Financial Conduct Authority imposed fines totalling more than $5bn on a group of US and European banks, some of whose employees were involved in attempting to manipulate the FX markets.

The penalties imposed on a number of international banks by the US authorities for violating international sanctions against Iran also demonstrate how a fraud can cross borders. Every case is different, but generally the fines often occurred as a result of the difficulty some non US banks have had in complying with U.S. law and/or possibly because some non US banks are under higher scrutiny that some US banks. This can be seen in particular with the BNP Paribas case. In 2014, the US Department of Justice imposed a fine of $9.6bn on French bank BNP Paribas after it pleaded guilty to violating US sanctions against Iran, Sudan and Cuba. The US authorities claimed that details had been removed from wire transfers so that they could pass through the US dollar clearing system without triggering red flags. Although the financial crime aimed to circumvent US sanctions, the focus of the fraudulent activity lay outside the US. However, the bank's presence in the US along with its use of the US dollar clearing system meant the crime fell within the US Department of Justice's jurisdiction. This is a contentious issue but one that we are likely to see frequently occur. In this case, French government officials repeatedly highlighted that BNP's alleged actions did not violate European law. However the US Justice Department felt that by operating in the U.S. (through Bank of the West and First Hawaiian Bank), BNP has agreed to follow US law. This case throws a spotlight onto the extra territorial jurisdiction (ETJ) reach of US law, which US officials may apply even when only a minor part of the transaction involves US banks[14].

And U.S. officials view sanctions violations seriously. (The violations do not have to occur in the country for American authorities to act.).

And these types of penalties have also been applied to banks in Africa. In April 2014, South Africa's central bank fined the country's four largest lenders a total of 125 million rand ($11.9 million) after finding deficiencies in their controls to combat money laundering and terrorist financing[15]. The penalties for FirstRand Ltd., Nedbank Group Ltd. and Barclays Plc's South African unit were 30 million rand, 25 million rand and 10 million rand respectively, according to the Pretoria-based South African Reserve Bank. The biggest penalty of 60 million rand was imposed on Standard Bank Group Ltd.

Earlier in January 2014, the U.K. Financial Conduct Authority imposed a 7.6 million-pound ($12.8 million) penalty on Standard Bank after saying its London-based unit didn't have adequate policies or procedures to protect corporate customers connected to political figures in relation to anti-money laundering.

To address these issues, a complete picture of a transaction is vital. Monitoring and sharing customers' transactions across businesses and jurisdictions facilitates the identification of any unusual transactions and behaviours. While most FIs invest in updating and validating their existing systems, a long-term approach should be adopted, rather than just aiming to meet today's set of minimum regulatory standards.

US$11.9m

fines to the four largest lenders in South Africa in 2014, for deficiencies in their controls to combat money laundering and terrorist financing

[14] Any authority can claim Extra Territorial Jurisdiction (ETJ) over any external territory they wish. However, for the claim to be effective in the external territory (except by the exercise of force), it must be agreed either with the legal authority in the external territory, or with a legal authority which covers both territories. ETJ may also refer to a country's laws extending beyond its boundaries in the sense that they may authorise the courts of that country to enforce their jurisdiction against parties appearing before them in respect of things that they did outside that country. This does not depend on the co-operation of other countries, since the affected people are within the relevant country (or their case is being heard by a court of that country).

[15] http://www.bloomberg.com/news/articles/2014-04-16/south-african-banks-fined-after-money-laundering-probe

Hacking

Hacking covers a huge variety of techniques used to find weakness in an organisation's IT security and so gain illicit access to computer systems for a range of reasons including fraud and data theft. In the Western world, the main issue with combatting hacking is a constant need to upgrade and maintain secure IT whilst simultaneously retiring legacy systems. However, many countries in Africa may provide a virtually blank slate. To give some global context, the US has a 78% internet penetration[16] whilst Nigeria, which has the highest levels in Africa, stands at only 29%. South Africa, with the largest economy on the continent, is currently at 14%. Mobility aside, with the African market so new, as IT levels improve African banks must be equipped to remain secure. Egypt in particular has seen a sharp rise cybercrime and Nigeria has a reputation for malware and cyber-crime, in particular the notorious 'Nigerian Prince' emails in recent years. Kenya also has a chronic hacking problem and general lack of internet security and this has now led to being addressed by the government. While South Africa's relatively under-developed infrastructure makes its high rates of cybercrime all the more alarming.

The Definition of Hacking

So what exactly is hacking? Hacking is a method of gaining personal details, often details to allow an individual to gain access to a customer's bank details. At its simplest, hacking may involve nothing more than attempting to guess passwords, an approach that is more likely to succeed against organisations with poor controls on password security and those that do not demand users change their password regularly.

Hacking can also involve attempts to induce users to divulge their account information using email-based "phishing" attacks, with information obtained from social media, or even fraudulent telephone calls that purport to come from the user's bank or financial services provider. Approaches such as these may simply involve gaining access to the victim's account in order to steal money but they can also provide the means to commit more intricate "identity theft", in which an individual's personal details are used to set up false accounts that are then used to obtain credit or make fraudulent purchases.

More sophisticated, technology-based types of hacking may involve attempts to introduce malicious software into the target organisation's computer systems, for example via email attachments, in order to capture sensitive information or to enable hackers to find a route into the system. The risks to cyber-security that hackers now pose have prompted the US ratings agency Standard & Poor's to warn in September 2015 that its credit ratings for banks will in future take into account the quality and strength of their IT security systems and procedures. "We view weak cyber security as an emerging threat that has the potential to pose a higher risk to financial firms in the future, and possibly result in downgrades," the agency said.

[16] World Internet Stats

Internal Fraud

Internal fraud is the most common way for banks to suffer losses. Estimates vary, but PwC's Global Economic Crime survey for 2014 suggests that 56% of fraud is carried out by employees, though this encompasses a wider range of sectors than just banking. Others put the insiders' share of fraud cases within banking as high as 70%[17].

And this is no different in Africa. In Kenya for example, cheque and internal fraud are the major risks that banks are grappling with in Kenya, where local lenders are increasingly being targeted by their own staff and IT workforce. Examples include collusion within IT operations operators who are able to delete logs after withdrawing customers' money. The recent crisis in Kenya's financial sector points to increasing cases of irregular reporting after bank management siphon customer deposits in webs of internal loans. This is highlighted by the recent Imperial Bank crisis where shareholders reported that the late managing director Abdulmaleck Janmohamed ran two sets of accounts with a vendor system. One was apparently regularly reported, not reflecting the true financial position of the bank, while the other, was not disclosed to the board and was comprised of fraudulent disbursements. This falsification of accounting statements meant that depending on who was the recipient, the most beneficial was given (similar to the case of Enron and Worldcom in the US that led to SOX legislation). Another example was where within a US based bank's regional office in Africa, an initial report indicated that Sh7.9 billion was extended in internal loans against banking principles.

These are just examples, employee fraud takes place at all levels of organisations. Survey data reported by the Economist Intelligence Unit show that among organisations that had suffered a fraud where the perpetrator was known, in 32% of cases the leading figure was a middle or senior manager while in 42% of cases it was a junior employee. In many cases involving banks, internal frauds will involve collusion between at least two individuals in order to circumvent the bank's controls, in particular the four eyes principle that is meant to ensure that one person carries out an operation while a second validates it. Employees with user privileges that give them high levels of access to the bank's IT systems, such as systems and database administrators, are particularly well placed to commit or facilitate fraud within banks and are often able to remove evidence of their actions from the system.

Fraud experts suggest that the process of carrying out a fraud usually takes place over a long period and will often start with an "exploration" of the bank's IT systems to see what the individual's access rights will allow them to do. They may look for a dormant account that will allow them to operate undetected or begin making small, temporary changes to the information on the system, such as a phone number, to see whether and how quickly they are detected. Criminologist Janet Goldstraw-White suggests that individuals who discover vulnerabilities in their employer's IT systems and control can feel "seduced" into committing fraud. "When they find out how easy this is, and get away with it, they often keep repeating the offence," she writes.

[17] ACFE 2014 survey

Addressing Internal Fraud

Whistleblowing mechanisms are now becoming common place in many organizations where staff members or any stakeholder can report any criminal acts anonymously. In East Africa (EA), KPMG has opened this service to companies in EA to subscribe and outsource the whistleblowing functions to KPMG. Fraud perpetrators tended to display behavioural warning signs when they were engaged in their crimes. The most common red flags were living beyond means, financial difficulties, unusually close association with a vendor or customer, excessive control issues, a general "wheeler-dealer" attitude involving unscrupulous behaviour, and recent divorce or family problems. At least one of these red flags was exhibited during the fraud in 78.9% of cases.

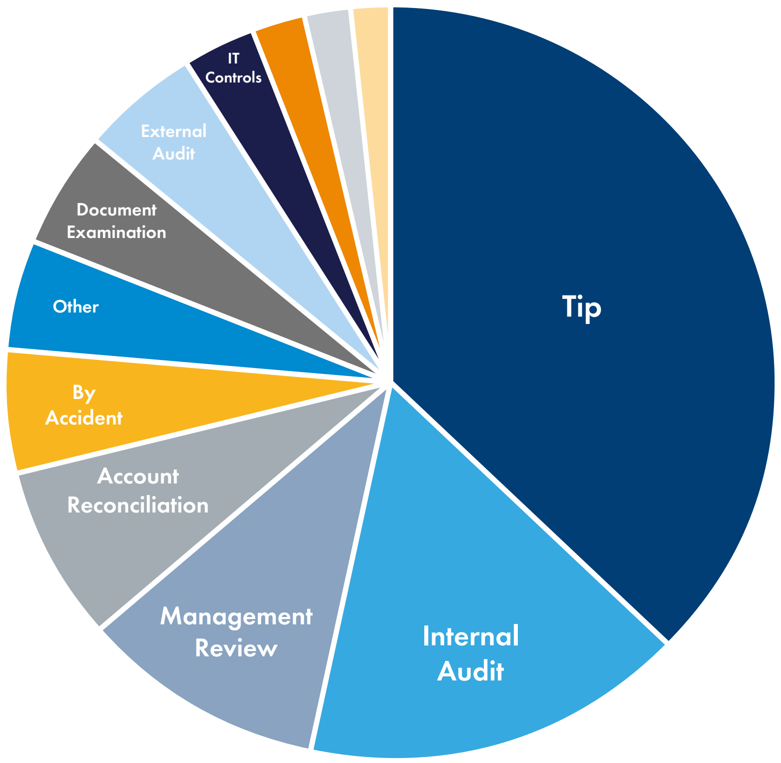
A recent survey of fraud in sub-saharan Africa revealed the most common way of detecting internal fraud. Worryingly the most frequent method of identifying the crime was through 'whistle blowing' or a 'tip' (see below for the results of the survey).

However, according to Association of Certified Fraud Examiners (ACFE) report (2016), the most prominent organizational weakness that contributed to the frauds in our study was a lack of internal controls. It cited this was the issue in 29.3% of cases, followed by an ability to override existing internal controls, which contributed to just over 20% of cases.

With the right system this can easily be addressed. Using forensic capabilities, transactions can be traced and identified when an FI's systems have been used internally to initiate fraud. Systems often use big data to continuously track human behaviour and detect suspicious activity before it becomes an incident, enabling banks to be proactive. These systems adopt a holistic approach, consolidating data in the same format and cross-referenced for maximum efficiency.

Automated frameworks could save on average 40% of the time financial institutions spend checking controls while also automatically monitoring controls continuously to facilitate audit reporting and applying new controls where required. This could result in time to implement a new control standard being reduced by 80% on average.

Detection Method by Region: Sub-Saharan Africa



Detection Method	Cases
Tip	37.3%
Internal Audit	16.2%
Management Review	10.2%
Account Reconciliation	7.4%
By Accident	5.3%
Other	4.9%
Document Examination	4.9%
External Audit	4.9%
IT Controls	3.2%
Notified by Law Enforcement	2.1%
Surveillance/Monitoring	2.1%
Confession	1.4%

Internal Fraud in Africa

Internal fraud is the most common way for banks to suffer losses and can take place at any level of an organisation. Roles with a high degree of access to IT systems, such as database administrators, pose a greater risk.

Who?

32%
Cases in which the leading figure was a middle or senior manager

VS.

42%
Cases in which the leading figure was a junior employee

Why?

Pressure
The employee's motivation to commit the crime, from personal problems such as drink, drugs or relationship breakdown to the need to out-perform colleagues or take revenge

Opportunity
Poor internal controls or the individual occupies a position of trust

Rationalisation
Fraudsters do not see themselves as criminals and so need to feel that their actions are logical and reasonable. They might argue they were "only borrowing" the money they stole or that their employer is corrupt

How?

Only 3.2%
of internal fraud detected in Sub-Saharan Africa is due to IT Controls

VS.

37%
of internal fraud within the region is through a tip (also known as whistleblowing), the most common method of detection

Many cases of internal fraud involve collusion between at least two individuals in order to circumvent the bank's controls

> **When they find out how easy it is, and get away with it, they often keep repeating the offence**
>
> Janet Goldstraw-White - Criminologist

Justice

There has been a significant increase in the number of fines and other punishments to banks and their employees for sanctions breaches and other financial crimes (see **G is for Global** for details of a recent fine for sanctions breaches). However, with the recent surge in Fintech technologies the range of breaches is likely to increase as regulators strive for justice. One such example is a fine of $700,000 against cryptocurrency company Ripple Labs[18] for failing to register as a money service business. FinCEN accused the company of violating the Bank Secrecy Act by failing to register as a Money Services Business while selling XRP and failing to set up an adequate anti-money laundering program. In 2013, FinCEN ruled that virtual currencies had to be properly registered with the US government and take steps to combat money laundering. In addition to the $700,000 fine, Ripple had to comply with all the rules and regulations set down by FinCEN for money-transferring companies, in addition to reviewing the last three years of its transactions for suspicious activity. The company must also submit to audits of its practices every two years until 2020.

Unfortunately, without the right policies and technology this trend of large fines is expected to continue into 2016. In fact, it is possible that an increase in personal fines may become common place. Banks (and individuals) may be forced to plead guilty to criminal charges and fire employees close to the issue. The recent fines are a clear indication that governments may reconsider the doctrine of "too big to jail" as fines levied in the past seem to have had little impact in curtailing illegal behaviour.

And these non-monetary penalties pale in comparison to an additional action regulators (particularly within the US) are talking about taking; suspending, at least temporarily, the bank's ability to move money. This level of suspension would impede the bank's ability to process payments or issue letters of credit for a period of time, causing significant disruption among its customers. And the combination of the fine and the potential additional penalties may damage the bank's credit rating.

> Recent fines are a clear indication that governments may reconsider the doctrine of **"too big to jail"**

[18] Ripple Labs built a payment transfer platform that people can use to move real or virtual money, and the company maintains its own cryptocurrency, called XRP II, which loosely compares to Bitcoin. (Unlike Bitcoin, XRP was fully generated before it went on the market, so an equivalent to Bitcoin miners doesn't exist in XRP.)

Know Your Customer (KYC)

There is a rampant increase in identity theft and identity fraud globally, and in particular within Africa. In South Africa alone, identity fraud increased by 16% to 3,873 cases in 2013[19] and costs the local economy an estimated R1 billion each year. With huge financial impact to a country's economy, regulation usually follows and banks must be able to support this through intelligent technology, but having the right systems isn't just about compliance. By gathering and understanding customer information (such as source of funds, type of business activity, expected sales volumes, linked or household accounts), institutions are aware of and better able to anticipate the level of customer account activity.

An important step in this direction is to follow strict Know Your Customer (KYC) and Customer Enhanced Due Diligence (CEDD, see also **C for Customer Due Diligence**) processes and procedures through which in depth customer details can be recorded and stored. This enables law enforcers and the regulators to have a money trail leading to the individuals or entities, in case of any wrongdoing. More significantly, as opposed to KYC and CEDD being considered necessary legislative evils, these elements enable banks to understand the customer activity and potential. It is a key benefit in proactively managing the customer relationship.

It has never been more important to have the right KYC solution in place to prevent identity theft, financial fraud, money laundering and terrorist financing. But standard KYC requirements are not enough to ensure protection.

Lexicon

A Lexicon is, from a computer programming perspective, the group of words that are used to create a programming language. A lexicon can be a branch of knowledge that stores all known words of a particular subject. For a sanctions screening system to function effectively, a wide variety of lexica for city-/country-connections and bank identifiers in various market networks, need to be considered. Effective software screening solutions use lexical analysis to match against not only country name variations, ISO country codes and deductions from city names, but also free text descriptions and financial identifiers. The solution must be sufficiently agile to spot even the slightest irregularity, utilising features such as 'relaxed pattern matching', where words are compared with a tolerance for approximation. Flexibility is key, as every institution will have its own needs, and rules may need to be applied according to requirements such as geographical area or business line.

Cultural differences are also important when screening for sanctions, particularly as these can be used to avoid detection. In many cultures, people may use four or five names, combining their given name and family names. Matching algorithms that fail to take into account these cultural differences result in gaps for FIs to fall through when the individual slightly modifies their name. Effective software should have good support for these cultural differences, capable of matching on portions of the name or name elements which are 'flipped' in order, and weighting them differently.

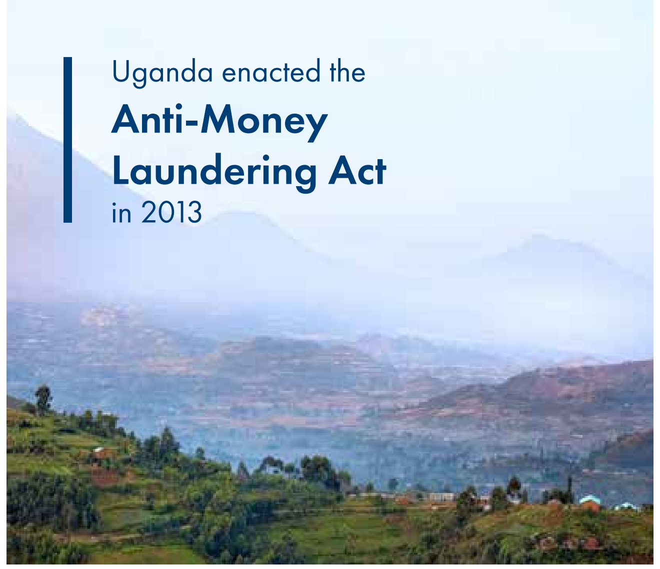
[19] Southern African Fraud Prevention Service (SAFPS)

Money Laundering

Money laundering in Africa is as rife as in any other developing nation. It is a hot spot for money laundering related activities, including the narcotics trade, smuggling, human trafficking and diamond dealings. In particular, in South Africa, the major financial centre in the region with its relatively sophisticated banking and financial sector, and its large cash based market, all make it a very attractive target for transnational and domestic crime syndicates. The South African Government (SAG) estimates that between $2 and $8 billion is laundered each year through South African financial institutions.

In general, the AML/CFT framework in Africa is still under development and has not yet reached the level of other regions. This is evident as at present only one African country (Algeria) is on the FATF list of non-cooperating countries and territories, however, South Africa, is the only African member of the FATF. The AML/CFT landscape in Africa is diverse and fragmented. While all African countries have established some legal provisions relating to AML/CFT, these are frequently not specialized stand-alone laws, but are rather embedded into general criminal offence frameworks, raising problems of their applicability to complex crimes. However, some countries have adequate protection; Mauritius for example, operates a financial intelligence centre to combat money laundering.

Uganda is one region that has more recently increased its focus on addressing money laundering. In 2013, the country enacted the Anti-Money Laundering Act (2013) to fulfil its international obligations, providing for the prohibition and prevention of money laundering. The offence of money laundering is created as an offence separate from other offences. The Act further creates the Financial Intelligence Authority as the body to spearhead the fight against money laundering activities. In line with international standards, the Act imposes duties upon various legal persons who might be used as conduits for money laundering and property that is obtained from the proceeds of money laundering is dealt with in line with the provisions of the new law.



Uganda enacted the **Anti-Money Laundering Act** in 2013

The same holds true for the implementation of measures; some countries have well-functioning Financial Intelligence Units (FIUs) while most countries are still struggling with problems regarding capacity, resources and law enforcement. Post-conflict or fragile political and governmental situations in many African states may also influence the crime situation and government efforts towards AML/CFT. In addition, due to the presence of informal financial services in many countries, criminal activities may simply move away from the official financial system into less regulated and supervised ones.

The meteoric growth in regional trade agreements and the inevitable complexity of exchanging $18 trillion worth of goods annually have created a perfect storm for trade-based money laundering (TBML). The fast growing threat of TBML exemplifies the many possibilities to launder money through manipulation of invoices, funnel accounts, lax regulations in high risk countries and miss-pricing of goods at import or export. According to the International Narcotics Control Strategy Report (INCSR) hundreds of billions of dollars are laundered annually by way of Trade-Based Money Laundering (TBML), although there isn't an accepted estimate of the magnitude and how much money is laundered through such schemes. But an example may show how low the risk is of TBML to be detected: in U.S. only about 5% of all imports and exports conveyed with vessels are actually controlled by U.S. Customs because of limited staff available to conduct such controls. TBML is one of the most sophisticated methods of cleaning dirty money, and respective red flags are among the hardest to detect.

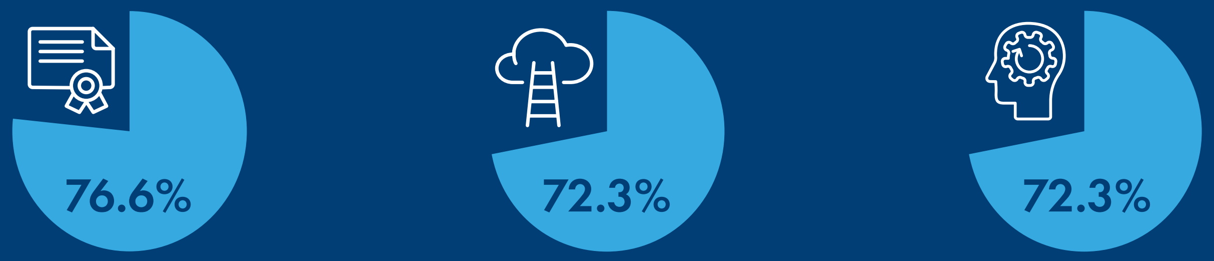
Another element that has an impact in combatting financial crime is of course the costs arising from AML/CFT measures taken. These are especially hard to bear for those institutions serving the poorest parts of the population, including microfinance institutions, cooperatives and rural/agricultural banks, and may hence hamper financial sector development. There are solutions available that are able to right-size for the requirements of specific institutions or sectors.

Money Laundering and Sanctions Screening in Africa

92% of financial institutions within the region state that money laundering is high risk[20]

88% of top global banks and financial services firms state that the Board of Directors takes an active interest in anti-money laundering issues[21]

3 main concerns by African FI's[22] with undertaking **Anti-Money Laundering**



76.6% lack of qualified resources

72.3% pace and impact of regulatory change

72.3% lack of overall training

Only 24.4%[23] of FI's in Africa utilise an automated customer risk assessment process, mainly due to their inability to record all relevant information in their customer data systems.

Only 77.3%[24] of African banks require customers classified as Politically Exposed Persons (PEP's) to evidence source of wealth and/or source of income

Many banks find it challenging to monitor PEP relationships and a large number of banks in the Eastern African region still rely exclusively on front office staff to identify PEPs

The former dictator of the Congo, Joseph Mobutu, is believed to have transferred up to $5,000 million from the country alone; with the right frameworks and software in place within the region this may not have been possible.

[20] KPMG Global Anti-Money Laundering Survey 2014 (Respondents came from a wide range of AML-related professional backgrounds across the financial services industry).

[21] KPMG Global Anti-Money Laundering Survey 2014

[22] KPMG Global Anti-Money Laundering Survey 2014

[23] KPMG Global Anti-Money Laundering Survey 2014

[24] KPMG Global Anti-Money Laundering Survey 2014

Near Real Time

To manage financial crime effectively (and particularly with the growing roll out of real-time payments), banks must be able to analyze every client interaction in real time. However, one of the greatest challenges to the effective use of big data analytics in detecting financial crime is the time required to process the vast volumes of information involved. Historically, sanctions screening and fraud prevention solutions have used real-time or NEAR REAL-TIME detection to prevent terrorist financing and financial crime; whereas anti-money laundering (AML) has primarily followed an "observe and report" process. Despite this approach being sufficient for regulators, international compliance teams are increasingly choosing to stop transactions before they are executed, based on suspicions of money laundering activity.

Besides gathering intelligence into large databases to support law enforcement investigations, a business argument for "observe and report" is that blocking transactions that are in fact legitimate will alienate good customers (see **F is for Four Eyes** and **W is for Wrong Person** for information on how this can be avoided). The alternative to the sophisticated use of software that enables a low false positive rate, is the extreme solution that some banks have selected by placing the onus on the suspects of criminal investigations to prove that their income is derived from legal sources (and if they cannot, it is assumed that it isn't). This clearly is not a feasible approach for the everyday business of banking, although asking questions about unusual transactions is smart business practice and is distinct from "tipping off" a criminal that they are under investigation.

Immediate Insight

Many banks currently run algorithms designed to detect fraud and financial crime on the data in their core banking systems quickly. The problem with this approach is that the data processing involved places a heavy load on the core banking system and will therefore tend to degrade its performance.

> One of the greatest challenges to the effective use of big data analytics in detecting financial crime is the **time required to process the vast volumes of information involved**

Oversight

Oversight of user activity lies at the heart of effective financial crime detection and deterrence. It is based on the ability to detect activities that either breach internal controls, resulting in a "red flag" alert, or to identify patterns of activity that do not in themselves breach controls but that taken together indicate the possibility of fraudulent activity. In both cases, effective monitoring of the use of the bank's technology systems by thousands of individuals and interpreting their behaviour is the key to effective fraud detection. Lack of reporting plus poor oversight can lead to incurring associated fines and risk reputational damage.

Late last year, the UK bank Barclays was hit by a £72m fine for failing to properly carry out anti-money laundering and financial crime checks on a major transaction in 2012 on behalf of ultra-rich clients[25]. No evidence of any crime was actually found, but the Financial Conduct Authority (FCA) said the bank did not carry out the appropriate checks to establish the purpose of the £1.88bn transaction, or to sufficiently corroborate the source of the funds from the clients who were said to be prominent people in public life. The FCA said that the bank went to "unacceptable lengths" to accommodate the clients and did so because it "did not wish to inconvenience the clients". But without the right level of oversight the impact could be even worse without the right processes in place.

> **Specialist IT auditors** have become a vital part of banks' armoury against fraud

Internal Fraud Oversight

From an internal fraud perspective, where employees in particularly sensitive jobs are concerned, specialist systems can be put in place to provide an added level of assurance in areas where banks have potentially serious vulnerabilities. In particular, specially designed systems are available to monitor the activities of systems administrators and database administrators on the bank's IT platform and reduce the risk of frauds carried out by system users with very high access privileges.

The critical role that technology now plays in anti-fraud oversight has also brought about big changes in the way that banks' internal auditors need to operate and the skills they require to do their jobs. Auditors are frequently drawn from the operational side of the bank and may therefore lack detailed knowledge of how the bank's IT systems work and their potential vulnerabilities. Specialist IT auditors have therefore become a vital part of banks' armoury against fraud and provide essential support for the work of the internal audit team.

Financial Crime Oversight in Africa

A number of measures have been adopted in Africa at both international and regional level to respond to the growing complexity and elaborate nature of financial crime methods. These initiatives have proved to be beneficial over time, however, a single approach to combat money laundering may not be fully effective due to the unique nature of the region's economies. It is therefore essential these countries are encouraged to concentrate on the fundamental threats and requirements and apply more comprehensive implementation efforts.

However, more success may be achieved if there is increased focus on international co-operation with each country. However, there is already a long list of international bodies that work to prevent and control money-laundering and terrorist financing and bodies such as FATF5, MENAFATF6, ESAAMLG7, GIABA8, UN9, IMF10, World Bank11 and Egmont Group12 etc.[26], there are still some sub-continental countries which are not part of any such regional or international bodies (see **R is for Regulation** for more information). These countries will benefit from applying their own oversight using technology that can apply these best practices and prepare them for when regulations are applied. In addition, where there is a strategy focused on adopting anti-money laundering policies that suit the states' economy as well as comply with best practices.

[25] Barclays fined £72m for poor oversight on financial crime, Telegraph Newspaper, 26 Nov 2015
[26] Southern African Fraud Prevention Service (SAFPS)

Financial Crime Oversight in Africa

Oversight of user activity lies at the heart of effective financial crime detection and deterrence. It is based on the ability to detect activities (through efficient systems or manually) that either breach internal controls or to identify patterns of activity that do not in themselves breach controls but that taken together indicate the possibility of fraudulent activity. Information within the industry dictate that Africa has some way to go in terms of ensuring robust oversight systems:

African FI's have the **lowest satisfaction** with their transaction monitoring system[27]

56% of FIs in Africa would like to see increasing international cooperation to facilitate consistency of approach to money laundering

Only 34% have personnel that are fully trained to understand and be aware of financial crime inhouse

Only 31% of organisations in the region carry out a fraud risk assessment annually and **22%** have never carried out such an exercise since 2014[29]

Only 35% of organisations in Africa have a fully operational cyber response plan[28]

Nearly 56% of all bank compliance staff in Africa have never received formal training[30]

Less than 5% of compliance staff have obtained professional certification[31]

27) KPMG Global Anti-Money Laundering Survey 2014 (3.12/5 for African and the Middle East)
28) Global Economic Crime Survey by PricewaterhouseCoopers (PwC)
29) Global Economic Crime Survey by PricewaterhouseCoopers (PwC)
30) 2015 AML Survey of Africa (ACCPA)
31) 2015 AML Survey of Africa (ACCPA)

Profiling

In cases where activities associated with financial crime do not involve a violation of any of the bank's internal controls, and therefore does not trigger a red flag alert on its security systems , PROFILING offers one of the most effective counter-measures. This aspect of big data analytics is akin to machine learning, in that the anti-fraud system will analyse large bodies of data over time in order to establish patterns relating to particular accounts and customers that reflect their normal behaviour.

The WEF 2016 report "The future of financial infrastructure"[32] identified 9 use cases across functions within financial services that would benefit from the distributed ledger technology DLT (see **B is for Bitcoin and Blockchain**). Especially Global Payments and Trade Finance which are especially vulnerable to fraud, money laundering and financing of terrorism, could drastically increase alert quality and benefit from reduced costs when banks and money transfer operators provided trusted and standardised dataset on DLT. Anything outside such DLT datasets might well be a suspicious activity.

In a simple example, this might involve payments into an account on a particular day of the month from a regular source such as an employer, withdrawals from ATM machines within a typical geographical area and purchases of a typical average size from a range of offline and online sources. By assembling data of this sort over a period, the system can create a notional profile of that customer or account against which to evaluate and query transactions that appear to fall outside of the recognised parameters.

These might involve an ATM withdrawal or card payment in a different country, a transaction of an unusual size or one that takes place at an unexpected time of day. In an investment banking context, profiling of the net positions and trading activity of a group of traders might enable a bank to identify whether any of them shows a pattern of activity that differs from colleagues working in the same team. Ultimately, the ability to create profiles in this way will enable anti-fraud systems to carry out ongoing predictive analysis of user behaviour and transaction patterns as they occur in order to give early warning of suspect activities.

Quantum

The quantum of financial crime is hard to determine precisely, since many cases go unreported. However, from a money laundering perspective alone, between 3-5% of global GDP is estimated to be laundered worldwide on an annual basis[33].

As the World Bank's World Development Report 2011 makes clear, financial crimes in Africa pose a significant threat not only to security but also to development[34]. And, according to the 2016 edition of the Global Economic Crime Survey by PricewaterhouseCoopers (PwC), Africa as a region experienced the largest increase in economic crime since 2014[35]. The study found that the prevalence of economic crime increased from 50% to 57% in Africa and financial services was identified as one of the main industries most at risk of crime within the region.

Overall, the survey by PwC found that the detection capabilities and response plans of businesses are not keeping pace with the level and range of threats now facing organisations. Only 31% of organisations carry out a fraud risk assessment annually and 22% have never carried out such an exercise since 2014. As mentioned, the region has seen an increased detection by means of whistleblowing hotlines and other detection methods however, according to the report economic crimes discovered by accident more than doubled from 6% in 2014 to 14% in 2016. And, from a cybercrime perspective, globally, only 35% of organisations have a fully operational cyber response plan and only 34 per cent have personnel that are fully trained. This is backed up by the ACCPA who state that 2015 AML Survey of Africa (ACCPA) show that nearly 50% of all bank compliance staff in Africa have never received formal training. And less than 5% of compliance staff have obtained professional certification.

Now that more and more capital flows into Africa, one cannot ignore the fact that the fight against financial crime has to be taken to another level in order to boost investor confidence in African markets and keep impetus in the FDI. These types of crime are only likely to increase if adequate controls aren't put in place. For example, some African states are noticing an increased spike in cybercrime when an area receives improved broadband connectivity (often without adequate defences), cybercrime spikes within a few days. The overall effect of the spike on global losses is limited, as the less developed countries do not generate the bulk of global income, but the regional effect is significant.

32) http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
33) International Monetary Fund 2014
34) World Bank, World Development Report 2011: Conflict, Security and Development, 2011
35) PwC's biennial survey interviewed 6,337 participants across 115 countries, most of them upper level executives: 45 per cent were C suite executives (chiefs), while 30 per cent were heads of departments or business units.

Regulators

Regulators in the majority of African countries have now become very involved in enforcing financial crime regulations. Ten years ago, compliance in many African states, was seen as a back office function, often integrated into either the legal department or internal audit, without its own identity. Compliance has now emerged as a profession in its own right,and is considered an important factor when managing a robust and effective Legal and Compliance Framework in a bank.

The most significant driver of this change has been the rapid increase in the amount of regulations and legislation that pertain to businesses, particularly in the financial services industry. Banks are starting to increase their focus on AML/CFT, not only as a result of the high fines that we have seen recently but also as soon we will see banks having to plead guilty to criminal charges and fire employees close to the issue (see **J is for Justice** which discusses the impact of regulatory breaches from a personal perspective). These non-monetary penalties pale in comparison to an additional action regulators (particularly within the US) are talking about taking – suspending – at least temporarily – the bank's ability to move money.

The impact of these fines (and this level of suspension) could impede a bank's ability to process payments or issue letters of credit for a period of time, causing significant disruption among its customers. And the combination of the fine and the potential additional penalties may damage the bank's credit rating. This increased focus was highlighted by a recent investigation by Nigeria's central bank and its financial crimes agency into banking deals after allegations of illegal transactions and has interrogated three top banking executives, officials and bankers in May this year[36]. Banking sources state that the probe saw three banking chief executives escorted from their offices and arrested for questioning.

Sources Available to Support Compliance

In terms of specific regulations within Africa, the Basel committee on Money Laundering and Terrorist Financing consistently issues general guides and expects banks in Africa and the rest of the world to adhere to them. It is noted that the US Fed generally requires banks who manage USD products to adhere to such minimum requirements such as AML and when non-adherence is noted, the affected banks will not be able to clear any USD related transactions through a US correspondent bank until they comply.

FATF calls on member States to adopt measures to freeze, seize and confiscate criminal proceeds, implement thorough know-your-customer processes, promote the reporting and monitoring of suspicious transactions in the banking sector, create whistle-blower protection, establish financial intelligence centres and promote cooperation in international law enforcement efforts. South Africa is the only African country that is a direct member of FATF. Some other countries are members through regional bodies such as MENAFATF, ESAAMLG and GIABA[37]. In addition, FATF also compiles lists of States that appear to be either high risk or non-cooperative jurisdictions. Algeria and Ethiopia are listed in the February 2014 as high-risk and non-cooperative jurisdictions. On a positive note, other African countries which are being monitored by the FATF but are consistently improving include Angola, Namibia, Kenya, Sudan, Tanzania, Uganda and Zimbabwe.

GABAC[38] is another regional initiative supporting financial crime mitigation but not an observer of FATF. The mission of GABAC is to lead, coordinate and boost actions undertaken by member States as part of the fight against money laundering and terrorist financing. It initiates and coordinates activities to assess money laundering mechanisms in member States.

In addition, some central banks within the region are taking regulation really seriously. The Central Bank of Kenya for example, has instructed bank auditors to probe financial statements as well as interrogate IT systems for risks. Sources state that some of the very big banks have just five risk assessment officers against their whole networks, and they go through samples manually.

Creative Compliance in Africa

From a general perspective, regulatory compliance is enabled through regular onsite bank visits to conduct surprise audits, analysis of financial information using advanced analytics, cooperation with their fellow regulators through frequent and structured engagements to build knowledge base and intelligence information.

Most African banks do not have a choice but to adhere to the expected minimum requirements. Regulators across the African landscape have now put in place legislations and mechanism to combat financial crime. Because monitoring isn't always possible, financial crime centres are being opened in various African countries e.g. FIC in SA, FRC in Kenya etc.. These centres act as a method in which any person can report suspicious activities touching on crime like AML, Terrorism, Unethical practices like tax evasion etc. Activities can be reported through channels such as hotline telephone numbers, email messages or on websites

There is very little research available on the subject of financial crime in Africa, however, KPMG's 2014 survey highlighted that 56% of respondents in Africa (and the Middle East) would like to see increasing international cooperation to facilitate consistency of approach. The survey responses indicated that financial institutions operating in this region would like their regulatory authorities to become more involved in the globalization of AML standards, learning from their counterparts in other countries to improve the regulatory approach in this region.

36) Finance: Nigeria's Economic and Financial Crimes Commission investigates banking deals, May 2016, The Africa Report

37) World Bank, World Development Report 2011: Conflict, Security and Development, 2011These groups are observers of FATF and aim to combat money laundering by studying emerging money laundering typologies, developing capacities and coordinating technical assistance focusing on international cooperation and they also assist African States in implementing the FATF recommendations through various initiatives in a form that suits that particular country.
38) Le Groupe d'Action contre le blanchiment d'Argent en Afrique Centrale (GABAC) - Central African Action Group against Money Laundering (http://spgabac.org/)

Sanctions

Africa has been far and away the target of more Sanctions from the UN, the European Union (EU), and the U.S. than any other continent. Most of these sanctions and related restrictions are aimed at resolving conflicts, and in recent years these have been overwhelmingly civil wars. While aimed at threats to international peace and security, sanctions have increasingly targeted individuals for gross human rights violations and in a few cases for leading unconstitutional usurpations of power, recognizing that these factors impinge directly on the intensity and duration of conflicts. Sanctions which have widespread international support prevent targeted states or individuals from evading sanctions or finding alternative sources of support to lessen their effect. The political and civil unrest within the region continue to pose challenges for financial institutions' sanctions screening systems in terms of responding to rapid changes to sanctions lists and increased volumes. The former dictator of the Congo, Joseph Mobutu, is believed to have transferred up to $5,000 million from the country alone, with the right frameworks and software in place within the region this may not have been possible.

The Challenges

Gaps and inconsistencies: A common issue with sanctions screening (and addressing money laundering) is that a system needs to allow for irregularities. In many cases, a financial institutions data will contain gaps and inconsistencies. These may have come from established clients whose data was not fully captured or not regularly reviewed and updated, relevant data spread across disparate systems or simply the inability to capture some types of information. However, the right software should be able to effectively screen the customer database, payments and other types of transaction and compare these against sanctions lists, while following the 'four eyes' rule as a default (see **F is for Four Eyes**). Even if a master customer record has been created to address these possible issues, without the right software to update this information it may quickly become outdated.

Wide range of variants: when screening for sanctions consideration must be taken in terms multiple names being used, the variety of languages or language specific country names (see **V is for Variants** for more information). Effective software screening solutions use lexical analysis (see **L is for Lexicon**) to match against not only country name variations, ISO country codes and deductions from city names, but also free text descriptions and financial identifiers. A sanctions screening solution must be sufficiently agile to spot even the slightest irregularity, utilising features such as 'relaxed pattern matching' where words are compared with a tolerance for approximation. Flexibility is key, as every institution will have its own needs and rules may need to be applied according to requirements such as geographic area or business line.

Geographic proximity: Geographical proximity to sanctioned countries such as Democratic Republic of Congo, Central Africa Republic, Sudan and Somalia which make it easy for transactions originating from these locations to find their ways into the economy.

However, screening for countries, and particularly, individuals within sanctions lists needn't be so challenging. In terms of the steps banks should take there are two elements that are essential: 1) having the right frameworks and 2) having the right technology to support those frameworks.

The Importance of Screening Frameworks

In terms of the framework, regulations stipulate that a sanctions compliance program be setup. This must meet the minimum requirements such as policies, procedures and internal controls to comply e.g. with the Bank Secrecy Act (BSA) for transactions involving US. These include verifying customer identification, filing reports, detecting suspicious activity, creating and retaining records and responding to legal requests. In addition, it is usually stipulated that a designated compliance officer be in place to assure daily compliance with the program and support other elements such as training and updating policies and procedures.

In particular, where an FI has a presence in more than one jurisdiction, it must adopt a group AML/sanctions policy. They should comply with the standards of the most stringent national frameworks and the territories where it has a presence (even through a subsidiary company). Customer centric regulations such as Know Your Customer (KYC) and Customer Enhanced Due Diligence (CEDD) must also be considered. FI's are required by law to establish well defined processes to meet global KYC/CEDD requirements and involves constant tracking of sanction/watch/embargo lists from around the world, along with being in constant sync with regulatory changes in different jurisdictions. These requirements vary across the geographic areas that their customers deal in; lines of businesses, product and service portfolios and delivery channels used by them; type and size of transactions undertaken by institution's customers and risk profiles that they belong to.

Screen Software Requirements

The evolving embargoed countries, sanctions regulations and complying with frequently updated lists mean that a highly agile, sophisticated software solution is essential. Best practice is that the solution should also follow the 'four eyes' rule as a minimum default. The software should be able to effectively screen a customer database, payments and any other type of transaction. It should then compare these against those names within sanctions lists issued by government departments within countries such as the Office of Assets Control (OFAC) in the US. Cultural and language variants must also be assessed against these lists within the system.

Software should also be sufficiently intelligent to identify when a transaction is matched up legitimately, yet there isn't a sanction applied. This is often referred to as a 'false positive' (**W is for Wrong Person**).

Technology

The rapid growth of mobile banking technology through phones and tablets reflects the central role that these devices now play in the lives of consumers around the world, and none more so that in Africa. Mobile banking activity is highest in Africa, led by Nigeria, South Africa and Kenya – which has the reputation for being the world's mobile money pace-setter with M-Pesa. There is more mobile banking activity than the global average of 66% – with engagement rates in Nigeria, Kenya and South Africa at 76%, 92% and 78%, respectively[39]. The example of an African bank that saw its customer base grow from 4m to 14m in less than two years after it introduced mobile banking is far from unique. Broadly Africans tend to use mobile to send airtime to other users, transfer funds and seek credit, however, Kenya has a massive use of mobile for banking.

The Threat of Mobile Technology

Landline-based telecoms and banking networks are expensive to build, which is one reason why only one in five of the world's 7 billion people have direct access to banks and financial services. But there are 5 billion mobile phones available globally that can be used as virtual wallets, or personal ATMs. By 2020, some experts predict, there will be 50 billion connected devices, and m-payments will most likely be the most popular form of banking in much of Africa.

The best example of m-Payments can be found in Kenya, where Safaricom launched one of the first mobile payment programs, called M-Pesa, in 2007. (Pesa means "money" in Swahili). As of January 2016, M-Pesa is used by 21.8 million Kenyans[40], with an average value of monthly person to person transfers on M-Pesa of Kshs 106bn (US$1mn). Of particular interest from a financial crime perspective, Person to Business transfers were at Kshs 23.5bn (US$232k) and Business to Person at Kshs 27.8bn (US$274k) per month. Its model is being imitated in more than 50 other countries, including much of Africa, Brazil, Afghanistan and India.

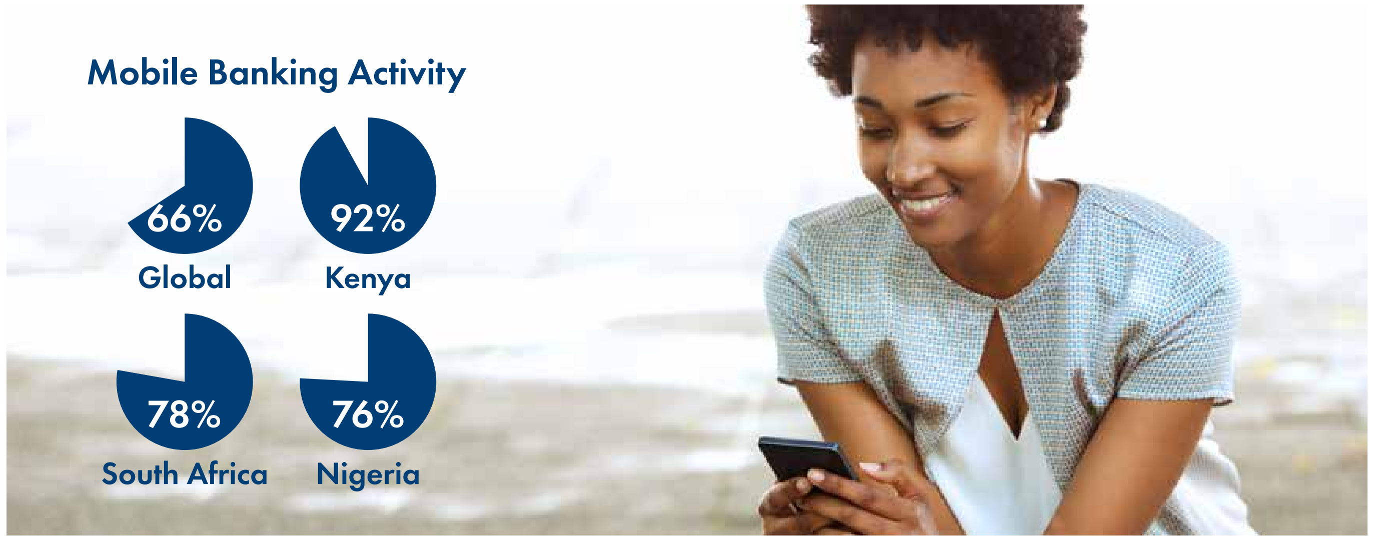
Thousands of street-corner shops in Kenya sell mobile-phone airtime, usually in the form of scratch cards. More than 60,000 of them have also registered as M-Pesa agents, far outnumbering Kenya's 840 bank branches. Annual transactions on M-Pesa are equivalent to over 20% of the country's GDP. Customers exchange cash for virtual value that goes into their phone, which becomes an electronic wallet or stored value card. They can then pay bills, buy things, transfer money and, importantly, receive credit on the card.

Besides being easy to use, it's usually cheaper than traditional money-transfer services. Foreign workers can be paid by phone, and then transmit the money to their family back home in seconds. Travelers can deposit lots of cash and then simply withdraw it in another country. Many big banks are now rushing to incorporate m-payments, and so are multinationals like McDonalds, Starbucks and Western Union.

Unfortunately, within most of Africa there are weak laws and enforcement against financial fraud and money- laundering. Customers often need little in the way of identification. The whole process often bypasses a country's financial reporting system. That makes it almost impossible for authorities to monitor m-payments, even if they had the expertise which they often don't (see Q is for Quantum).

Addressing the Threat

The huge popularity of this new technology places immense pressure on the banks' IT systems as transaction volumes explode, as well as providing another route into the banks' information systems that can become vulnerable to fraud and unauthorised use.

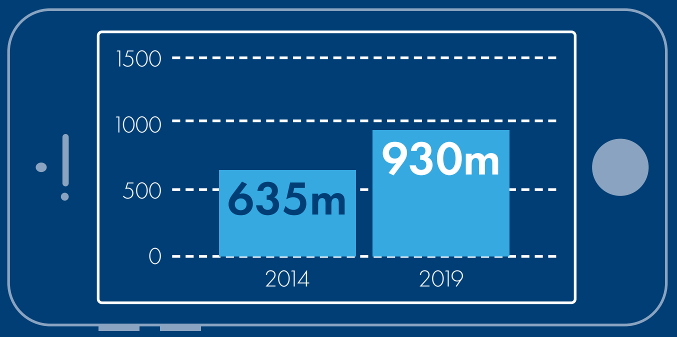


[39] MEF mobile banking report 2014
[40] https://en.wikipedia.org/wiki/Safaricom - September 2016

Technology and Complexity in Africa

The rapid growth of mobile banking technology through phones and tablets reflects the central role that these devices now play in the lives of consumers around the world, and none more so that in Africa. However, these new channels make it harder for banks within the region to have a clear overview of all the activity taking place on their systems.

Estimated rise in mobile subscriptions & level of interest in mobile banking



58% of sub-Saharan Africa mobile users are interested in using mobile banking and mobile wallets[41]

Risk
IT security becomes more complex as new information systems are implemented on top of older ones. This builds up layers of technology that do not necessarily link together well and are hard to police

Benefit
Because mobile banking is largely customer driven and fully automated, its growth should help to reduce banks' exposure to fraud – particularly that carried out by insiders...

Risk
Even a relatively small institution will have multiple databases running on different servers that are accessible to a large number of staff – and people are the weakest link

... But
Straight through processing, where there is no human involvement in a transaction, puts huge emphasis on the effectiveness of internal control systems

[41] Ericsson Mobility report 2015

User Behaviour Analytics

User Behaviour Analytics (UBA) is a fast-emerging area of fraud detection within banks. It is based upon big data analysis and requires the ability to assess very large volumes of data from multiple sources within the bank's IT systems. This is analysed at the level of individual users and banks also seek to identify links between users and entities on the system. Once the UBA system has been configured to reflect the working practices of an institution and has established a baseline for its users' typical behaviour, it is able to identify anomalous examples, whether carried out by insiders or external intruders, and flag them for further investigation.

This area of financial crime detection is still developing and to date has varied significantly from one provider to another. The important trends in this market include the level and extent of data analysis that the bank is required to carry out internally. More advanced UBA systems now include large suites of so-called "canned analytics", meaning that the system provides information to the bank in a readily useable form, for example via dashboards. Banks therefore do not require their own data scientists in order to make proper use of it. UBA providers are also increasingly providing these systems as a service, whereby the provider's staff carry out analysis and forward reports of anomalous activity to the customer.

From a regional perspective, a recent report[42] indicates that the African market is somewhat behind on adopting this approach. The report segmented the global User and Entity Behaviour Analytics Market into North America, Asia-Pacific (APAC), Europe, the Middle East & Africa (MEA), and Latin America. The North American region is estimated to lead the global User and Entity Behaviour Analytics Market in 2016 by accounting for the largest share in the global User and Entity Behaviour Analytics Market. The Asia-Pacific User and Entity Behaviour Analytics Market is projected to grow at the highest CAGR during the forecast period, 2016 and 2021. Some of the factors, such as rapid growth in the usage of web and mobile applications in the Asia-Pacific region and the need to protect these applications from vulnerabilities have resulted in increased demand for user and entity behaviour analytics solutions that identify security gaps in the network infrastructure and web and mobile applications, and help in addressing them. Given the fast growing adoption of the use of mobile, if web infrastructure developments within the region were to progress further than expected then it is quite possible that UBA may reach the same level as Asia-Pacific.

Variants

Anti-money Laundering (AML) and sanctions screening software needs to be sufficiently nimble to adapt because an FI's client profile often has many variants and is continually evolving.

Name Variants:

In many cultures, people may use four or five names, combining their given name and family names. Matching algorithms that fail to take into account these cultural differences result in gaps for financial institutions to fall through when the individual slightly modified their name. Effective software should have good support for these cultural differences, capable of matching on portions of the name or name elements which are 'flipped' in order and writing them differently.

Many Languages:

For a system to function effectively other factors such as the wide variety of languages used or country names, need to be considered. Effective software screening solutions use lexical analysis (see L is for Lexicon) to match against not only country name variations, ISO country codes and deductions from city names, but also free text descriptions and financial identifiers. A sanctions screening solution must be sufficiently agile to spot even the slightest irregularity, utilising features such as 'relaxed pattern matching' where words are compared with a tolerance for approximation. Flexibility is key, as every institution will have its own needs and rules may need to be applied according to requirements such as geographic area or business line.

In addition to using sophisticated software to pick up on these variants, a flexible workflow management framework can be used. This should have the ability to respond to changing customer profiles, changing types of transactions and new legislation.

[42] User and Entity Behaviour Analytics Market by Type (Solution and Services), Deployment Type (On-Premises and Cloud), Vertical (Financial Services & Insurance, Retail & Ecommerce, Energy & Utilities, IT & Telecom, and Healthcare) - Global Forecast to 2021, published by MarketsandMarkets

Wrong Person

False positives (or the identification of the wrong person) occur when a transaction is matched up legitimately, yet there isn't a sanction applied or an incident of money laundering. Resolving these hits costs time and money, and may cost banks good customers. The challenge is that there are so many common names on the lists that many normal, potentially good customers may be treated unfairly unless they are identified as 'false positives' quickly and addressed effectively. It is therefore essential that software with a very low 'false-positive' alert rate is used, to ensure minimal disruption to the FI and its customers. Software may use information such as address, date of birth, mother's maiden name, passport number, or further historical trends that can help clear these hits quickly.

X Border Fraud

Reports show that the developing world lost US$6.6 trillion in illicit financial flows from 2003-2012[43]. And South Africa alone is known to loose roughly an average of $12 billion every year[44]. The impact to the African economy is huge; to reach critical development goals, Africa's emerging market can ill afford to lose funds through tender fraud, money laundering and other forms of corruption; yet this loss of funds is at an all-time high and is increasing.

Technology enables banks to operate with very high transaction volumes, but the same is also true of fraudsters. This means that a single fraud can have an XXL impact, resulting in huge losses. In one extreme case of ATM fraud uncovered in the US, a criminal gang looted $45m from cash machines around the world in two separate attacks. The gang first hacked into databases containing details of prepaid debit cards belonging to two banks based in the Middle East. The hackers collected debit card data, removed withdrawal limits on the accounts and created access codes. They were then able to use the account data and fraudulent access codes to enable any plastic card with a magnetic strip to withdraw cash from the compromised accounts. In their second, much larger attack the gang passed information to groups of fraudsters in cities around the world who then moved from one ATM to the next, withdrawing huge sums. In the space of just a few hours, more than 36,000 fraudulent withdrawals were made resulting in the theft of about $40m.

Information on the theft became public when eight members of the New York-based cell involved in the fraud were brought to trial. The case highlighted a range of vulnerabilities that the fraudsters were able to exploit, including the lack of security and screening technology at the banks involved that could have helped them to detect and counteract the hackers. Also, the continued use in the US of cards with magnetic strips enabled fraudsters to produce working versions using false access codes very easily. These magnetic cards have been abandoned in most other countries and are now being phased out in the US as well in favour of chip-and-pin technology, which is more difficult to copy, but because US banks and merchants still used magnetic cards they continued to be accepted in other parts of the world.

US$12bn
per year, on average,
lost in South Africa to
illicit financial flows

[43] The Illicit Financial Flows from the Developing World: 2003-2012 report by Global Financial Integrity
[44] http://www.deloitteblog.co.za/how-financial-criminals-make-an-impact-on-your-business-and-the-south-african-economy/

Youth

In the past two decades the rapid spread of the digital economy has exponentially increased the quantities of data that organisations generate and with it the challenges of maximising the value of these vast pools of information. In January 2009, Hal Varian, Google's chief economist, told McKinsey Quarterly: "I keep saying the sexy job in the next 10 years will be statisticians... The ability to take data – to be able to understand it, to process it, to extract value from it, to visualise it, to communicate it – that's going to be a hugely important skill in the next decades." Financial crime mitigation technologies that depend on these crucial skills are still in their youth – many were developed only in the past few years and in many cases banks have only recently begun pilot projects that use modern techniques such as big data analytics. There is much further to go before these technologies become a routine part of how banks operate day-to-day: in early 2014, the technology market analyst Gartner said that just 8% of large, global companies had adopted big data analytics for at least one security or fraud detection use case. It forecast that the proportion would increase to one-in-four by 2016.

These new technologies are developing quickly, which brings both opportunities and challenges for organisations that want to take advantage of them. On one hand, the rapid evolution of systems will require banks to adapt and update their controls frequently and undertake continuous training to stay abreast of technological developments and the evolution of techniques for committing fraud. On the other, as anti-fraud systems evolve they are continuing to improve. Increased processing power is enabling them to become faster and more intelligent, and the quality and user-friendliness of the analysis they provide to security staff are improving, making them easier to use. Banking is becoming ever more dominated by digital technologies and as this process continues, technology will inevitably be an indispensable weapon in the constant fight against fraud.

Zero Day

The battle between institutions and fraudsters resembles an arms race. Technology developers are at work on both sides: hackers creating new ways to penetrate IT systems to steal information and carry out fraudulent transactions, while software vendors work to block these attacks and discover new vulnerabilities in their programs before the hackers do.

Occasionally, hackers succeed in exploiting holes in the software systems that organisations use before IT security staff become aware of the weakness. These are known as zero day attacks and refer to the taking advantage of a previously unknown software flaw. There have been zero day attacks on widely used pieces of software including PC and Mac operating systems and web browsers. Software vendors release thousands of security patches to plug the holes that are discovered in their code, but in some cases they are discovered only when people suffer an attack.

It can take years for a zero day attack to be discovered. The Red October malware went undiscovered for five years, during which time it was used to steal information from governments, embassies, energy companies and nuclear installations in 39 countries. It was uncovered in October 2012 by the Russian security company Kapersky Labs. The creators planted the malware in Microsoft Word and Excel documents that were sent to target recipients by email.

However, although these security breaches are a cause for concern, technology continues to develop quickly and the security that surrounds the IT systems that form the critical infrastructure of banking is becoming stronger all the time. Major advances in areas such as big data analytics and real-time monitoring mean that unauthorised activities can be detected and dealt with more quickly than in the past, and the arrival of predictive analytics promises to increase the strength of the defences that banks can rely on still further. The ability of technology to provide effective protection against fraud has never been greater than it is today – and it is improving all the time.

Author

Emma Wadey
Product Strategy
Temenos France SAS

With special thanks to

John Kiptum
Risk Consultant
NetGuardians Africa

About Temenos

Temenos AG (SIX: TEMN), headquartered in Geneva, is the world's leader in banking software, partnering with banks and other financial institutions to transform their businesses and stay ahead of a changing marketplace. Over 3,000 firms across the globe, including 41 of the top 50 banks, rely on Temenos to process both the daily transactions and client interactions of more than 500 million banking customers. Temenos offers cloud-native, cloud-agnostic front office and core banking, payments, fund management and wealth management software products enabling banks to deliver consistent, frictionless customer journeys and gain operational excellence. Temenos customers are proven to be more profitable than their peers: over a seven-year period, they enjoyed on average a 31% higher return on assets, a 36% higher return on equity and an 8.6 percentage point lower cost/income ratio than banks running legacy applications.

Learn More

To find out how Temenos can help with your digital banking needs, contact sales@temenos.com or visit us at www.temenos.com

About Netguardians

Netguardians is a leading banking software company recognized for its unique approach to fraud and risk assurance solutions. Our award-winning software leverages Big Data to correlate and analyze behaviors across the entire bank system – not just at the transaction level. This broader vision is the secret to our creative edge. We earn the confidence of our clients by combining the technical know-how of our R&D team with our in-depth understanding of the evolving risk challenges faced by banks in a border-free world.

Founded in 2007, NetGuardians was the first company to emerge from the innovation incubator Y-Parc, in Yverdon-les-Bains, Switzerland. The company now enjoys a solid international presence with a steadily growing clientele in Europe, Middle East and Africa. In 2015, NetGuardians has been named a Gartner "Cool Vendor" in "Cool Vendors in Audit and Compliance Innovate Controls Validation Techniques": http://www.netguardians.ch/gartner

TEMENOS
THE BANKING SOFTWARE COMPANY

NetGuardians