

Doing Business in a War Zone: Somali Banks and

Key findings:

1. Banks and telecoms companies are ready and able to implement higher compliance and regulatory standards, but the government is too weak to design and implement them.
2. Although the telecoms companies are accused of refusing to implement the provisions of the Telecoms Act, the key unimplemented rules require government action, principally the adoption of a national identity system and an improvement in security.
3. The telecoms companies have adapted to the security situation in Somalia to grow their businesses and have disallowed location services and metadata collection.
4. Telecoms companies make it difficult to retrieve call logs data, even by users, in order to avoid local politics making the same requests.
5. Telecoms companies and banks are not believed by the National Intelligence and Security Agency (NISA) to make pay offs to terrorist groups.

Summary

Business in Somalia is shaped by security and governance issues. Major businesses in the country started their journey during the darkest days of the civil war. They adapted to the situation and helped lay the groundwork for the recovery of the Somali state by building bridges across clan borders. As the country enters its third decade of internal strife, Somali businesses continue to grow, many on a global scale. They are now subject to local, national, and global forces.

This paper is the result of interviews with more than a dozen business leaders and senior government officials. The aim was to understand how major Somali businesses have fared in the new business climate, with the passage of the anti-money laundering and combating the financing of terrorism (AML/CFT) bill of 2016 and the 2017 National Communications law. Specifically, we wanted to know whether the

businesses have complied or not and the reactions of other actors to the new regulations.

We found that major businesses proactively complied with the laws; most did so on their first day of operation. Banks had strict Know Your Customer and due diligence systems in place from the outset, before the government required them to do so. Being part of a globalised economy, they complied with global standards even if the government did not require them to do so.

Data protection and privacy was also looked at in order to identify loopholes and space for improvement. We found that local considerations had created a culture of cautiousness when it came to data retention and access. The businesses are years ahead of the government in this regard; Somalia has no data protection law, and none seems to be in the works.

The Banking Sector

There are five major banks in Somalia: Salam Bank, Amal Bank, Dahabshiil, Premier Bank, and IBS. The first bank to be created in Somalia after 1991 is Salam Bank (SB), which was officially launched in 2009. As it existed before any national banking laws and regulations were created, it had to comply with international banking standards in order to be able to do business globally. Due to the nonexistence of national banking regulations, most Somali banks based their policies on the Financial Action Task Force guidelines (FATF) before the adoption of the Somali AML/CFT law in 2016. The AML/CFT law is helpful in gaining international legitimacy for the banks; they are more than happy to fully comply. The government assumes that Al Shabaab (AS) is unlikely to hurt the banks for complying because it does not hurt them for paying government taxes.

Without being required by Somali law, SB demanded that account holders provide passports and company registrations before opening accounts. The public was resistant to its registration systems and SB was

instrumental in making them accept it; in the beginning they were accused of being spies for demanding biometric data to open bank accounts.¹ Likewise, IBS has one of the most stringent requirements for opening a new account, requiring that customers provide fingerprints to the bank; it also searches OFAC lists to ensure that people creating accounts are not subject to international sanctions.²

Having built their businesses in an environment without a functioning bureaucratic government, some individuals have amassed large fortunes without registering their companies. When told to register companies, they are very resistant and suspect that the banks are in cahoots with the registration ministries.³

All the banks are involved in some way or another in providing financial services to the government, including payroll services and the collection of fees for the government. Despite this deep interaction with the government and material support for it, they have not been threatened by AS. This is because the group does not punish providers of public services for providing the same services to the government. That is why it targets building contractors who build offices for the government but not those who build roads because the latter are used by the public.⁴



Banks proactively submit to audits for compliance purposes. However, they are concerned about the government's ability to protection of the data they share with it, and the retributions they may face from terrorist groups if the data is leaked. The banks' concern is rooted in their experience with government officials in the past and the current power struggle between the Financial Reporting Centre (FRC) and the Central

Bank of Somalia (CBS).

The FRC and the CBS

The AMLF/CFT law makes it clear what both institutions have to receive from the banks; however, the CBS seems to require banks provide it with the same data they provide the FRC. Banks were confident in the ability of the CBS to protect the data they shared with it; while they demanded that the FRC create secure networks with which to share compliance data, they did not make the same request of the CBS, suggesting that it has more to do with trust in the CBS as an institution than a fault by the FRC. While the FRC was in the process of creating secure information systems during the research for this paper, bank executives perceived that the FRC has neither a system nor a user control mechanism to restrict and log what each individual has accessed or printed.⁵ On the other hand, the CBS is well respected by the banks; they have confidence in the ability and qualifications of CBS staff, according to half a dozen executives from different banks. This may have to do more with the history of dealing with the CBS than anything inherently wrong with the FRC. The banks are confused by the power struggle between the two institutions and seem to have chosen a favourite in the struggle.

Furthermore, there are confusions and issues over who is supposed to be the compliance agency –whether it is supposed to be the FRC or the CBS. Interviewees in the CBS said that it was unclear where the FRC fits into the reporting structure and whether it should report to the CBS or the finance ministry.⁶ As a result of the confusion created by the two regulating agencies claiming oversight responsibility and to be on the safe side, banks are forced to send suspicious transaction reports to both the FRC and the CBS. In order to reduce confusion, banks are currently being trained in the compliance procedures by the FRC.⁷ Nevertheless, some banks understand the law and send different reports to the FRC and the CBS; others are forced to send both suspicious and large transactions reports to both the FRC and the CBS.⁸ As the banks proactively comply with the regulations, both the FRC and the CBS are happy with the level of cooperation they receive from the banks, and considers them compliant

- 1 Interview with Salam Bank executive, December 2018.
- 2 Interview with an IBS executive, December 2018.
- 3 Interview with Salam Bank executive, December 2018.
- 4 It however targets contractors building roads where it does not want roads.
- 5 Ibid.
- 6 Interview with a CBS official, December 2018.
- 7 Interview with senior FRC official, December 2018.
- 8 Interview with multiple bank executives in Mogadishu, December 2018.

with the AML/CFT law.

Telecoms

The largest telecom company in Somalia is Hormuud, which claims to have 75% market share in south and central Somalia with 50% of its users being in Mogadishu. However, other telecoms companies accuse it of having an even larger share and using its local influence to its advantage. Hormuud was established in 2002 by local businessmen and employees from the ashes of Al-Barakaat. It works in south and central Somalia and partners with Golis and Telsom. Hormuud started working before the existence of a Somali government; it was forced to adapt to the business and global political climate before the government regulated its work.⁹ The security in the 1990s was predictable and according to clan boundaries. The telecoms companies were essential in ridding the country of clan boundaries by forcing companies to work across clan lines and build lasting presence across said borders.¹⁰ Security was always and still is the most expensive service that telecoms companies incur. Technicals were necessary for movements of company officials and supply trucks. As a result of the clan boundaries, employment of locals in every station was necessary and demanded by the local elders.

Because there was no government, the telecoms companies had a unified office used as a clearinghouse that acted as a sort of governing body. It set calling fees between the companies and allocated frequencies. However, telecoms companies currently do not have a way to call one another because the unifying body was disbanded as a result of competition and a lack of trust among the companies.

Insecurity and lack of unified governance is expensive for business as major companies are required to comply with different rules across a small geographic area. For instance, a Hormuud truck is asked to pay illegal extortion at multiple points between Mogadishu and Afgoi.¹¹ Likewise, the government is too weak and absent to protect Hormuud masts in the border regions with Kenya, where cross border attacks by Kenyan troops regularly demolish masts owned by the company.

To make matters worse, there is no top-level government statement about a private company being attacked by a foreign power. Hormuud says it has lost millions in the Kenyan attacks.



As the largest telecom, Hormuud faces the most pressure from all actors in the Somali conflict. For instance, AS stops the company from building new antennas and harasses its supply trucks. Likewise, all security actors -- AS/FGS/FMS/AMISOM-- sometime switch off Hormuud antennas along the entire routes when convoys are moving. Some regions in Hiran have daily interruptions of up to 5 hours by AMISOM. The interruptions affect millions of customers and cause the loss of millions in revenue every year.¹²

The Telecoms Act of 2017

In 2017, the telecommunications bill was finally passed by parliament and signed by the president. It created a regulatory agency for the telecoms industry and required the registration of all SIM cards in the country. The companies had been opposing the passage of this law for years. They feared the government and distrusted giving information to people whom they did not know. They believed that government officials are all diaspora and are unaware of the true situation in the country; that they have no understanding or a viable solution to issues specific to Somalia.¹³ For businessmen used to dealing with local actors, the federal government and its laws were too scary to stomach. Hormuud is accused of having being the main obstacle to the passing of the telecoms act. It maintains that it was never opposed to the telecoms law, which took a decade to pass the parliament; it says that the instability of the FGS executive was responsible for the delayed passing of the bill.

The National Communications Authority

The NCA is the regulatory body responsible for implementing the National Communications Act of 2017. It is tasked with the protection of customer rights and promotion of fair business practices.

9 Interview with a Hormuud executive, December 2018.

10 Interview with Nationlink executive. December 2018.

11 Interview with a Hormuud executive, December 2018.

12 Ibid.

13 Ibid.

However, telecoms companies that were not included in the BoD of the NCA accused Hormuud of indirectly controlling the individuals in the NCA. Nevertheless, the NCA accepts that Hormuud had a bigger say in the selection of the BoD because of its size in the market; consultations were held based on market share.¹⁴

The telecoms companies fought against the law and worked to block its passage for years because of two main concerns: the entry of foreign companies into Somalia and the lack of national IDs. They finally accepted it in its current form after their two concerns were addressed. Their concern about foreign investment was addressed by the Investment Act of 2016; likewise, the ID issue was addressed after talks between the government and telecoms companies in which both sides agreed to postpone implementing that provision until there was a national ID.¹⁵

NCA will require telecoms companies to get new licenses from January 2019; this would formalise their numbering system and the frequencies being used. The self-declared independent of Somaliland creates more problems for companies, but in the end they would have to need to register in order to use the national numbering system.

Registration

The biggest hurdle to the telecoms bill is the lack of national IDs and the absence of government authority from most of Somalia. If the government were to create national IDs in the current situation, it would still be impossible for the telecoms companies to register people outside major population centres, forcing them to cease operations in large swathes of the country. Telecoms are willing to follow the rules, but it is impossible for them to implement a rule requiring them to register SIM card users while the country has no national ID system; the FGS has to do its part in terms of registration of SIM card holders; it has to create national ID cards.¹⁶ While the telecoms companies have excellent relations with the government and adhere to its regulations, these companies feel that the FGS has failed in its duty of providing security to the country and improving the business climate.¹⁷

Lack of national IDs also affects the banking sector; it impacts financial injection capacity and creates a small percentage of people who can open bank accounts. For instance, an online banking system was switched to be

14 Interview with NCA official, December 2018.

15 Interview with an NCA official, December 2018.

16 Interview with a senior Somtel official, December 2018.

17 Interview with a senior Somtel official, December 2018.

18 Interview with an IBS executive, December 2018.

19 Interview with Salam Bank executive, December 2018.

based from dollars to Euros following U.S.

demands that Somalia have a national ID system if dollars are to be sent and received.¹⁸ The lack of a national ID not only hurts the banks' ability to gain more customers, it also hurts those who already have bank accounts that they cannot fully utilise for international trade.

Mobile money

In 2009, Hormuud, Golis, and Telesom introduced mobile money into Somalia. It was known as Zaad by Hormuud and Telesom, and Sahal by Golis. In order to open an account, users were required to provide real names, a guarantor, and a photo was taken by the companies. Users had the ability to use their SIM cards as banks, with the option to raise the limit of their accounts to as much as they wished. Shortly after launching, actors in Mogadishu started opposing the requirements needed to open a Zaad account. Hormuud's Zaad required people to give biometric data to use electronic money; it was considered suspicious by the public.¹⁹ Taking photos was later discontinued, resulting in Hormuud curbing the limit of Zaad to \$700 to make it a petty cash account. This was not enough for Al-Shabab, and it outright banned Zaad in 2010.

In 2011, Hormuud introduced EVC+ without much advertisement. It was based on another system, EVC, which was used to transfer airtime credit from one phone number to another. Creating an EVC+ account is a simple process that any user can do from their phone; the limit is \$150 when created this way. Expanding it to \$300 requires the user to provide their real full names. This becomes relevant when the user attempts to link their EVC+ account to the bank using the Deqton service. This would require they provide an FGS/FMS-issued ID or passport and have their photo taken by the bank. EVC+ in its original form is therefore a small petty cash account; expanding it beyond petty cash does not break the AML/CFT regulations as the users would be required to provide official identification.

Golis and Telesom still maintain photo and guarantor requirements for opening a mobile money account. They also still have unlimited ceiling to mobile money accounts; users can request their account limits to be expanded to whatever amount they want as long as they have the money to fill it. While users can be identified and their accomplices traced in the guarantor system,

the ability to send and receive large transactions has proven to be a suitable tax collection method in AS Sharqistan -- AS in Puntland. As the group lacks a suitable area to force businessmen to bring it taxes as it does in the south, businessmen are asked to send taxes to Sahal mobile money accounts.

Some banks feel that the EVC+ is an obstacle to the growth of the banking sector as it favours one bank over others; only Salam Bank can be utilised to move monies to and from EVC+. Likewise, Hormuud does not allow other banks to use its automatic messaging system; for instance, IBS is forced to use a texting company in Singapore in order to send text messages to its users as Hormuud does not allow Salam Bank competitors to use its services. IBS is hopeful that the NCA may force Hormuud to change its conduct.

The CBS is yet to adopt a position on mobile money, although at least \$100 million is kept as mobile money any given day.²⁰ Mobile money regulations are in the consultation stage. Proposals being considered include requiring that telecoms keep the mobile money in circulation as physical cash in the bank.

Interconnectivity

Regulations governing interconnectivity that are under consideration by the NCA support the continuation of the status quo where users cannot call one another across networks. It gives too much leeway to the telecoms companies by giving them a free hand to negotiate pricing and other conditions. If the telecoms companies had the will to interconnect, they would have done that a long time ago.

Data protection

The telecoms industry existed before any government system; Mogadishu alone had more than a dozen zones ruled by warlords who were the ultimate authority in their area. Telecoms companies understood that they needed to have strict data protection policies in order to survive in the security situation in Somalia. Yielding to data sharing demands from one actor would open the company up to retribution and similar demands from other actors. Information sharing is complicated by the security situation in Somalia. If it became public that they share info with one entity, all entities would demand access to data. All telecoms log incoming and outgoing calls, but place restrictions on customer access to call logs. Only top-level executives have access to call logs after a certain period. Branch managers have access to data that customers would need on a

daily basis, such as mobile money transactions. For instance, info on EVC+ is retained by the system for at least two years but can be seen only by top executives. Basic info on recent one-month to three-month EVC data can be shown to the users. Special officials in each Hormuud office have access to EVC+ and its data for up to three months. However, although AS has never officially demanded information, AS individuals have directly approach Hormuud individuals for data. When the approached individuals reject AS demands, the AS persons retaliated by trying to disrupt the company's sites.

Likewise, although banks have access to financial data that would be useful to AS in its taxation plans, no bank has been officially requested by AS to provide financial data belonging to its customers. Banks make it difficult for anyone but the account owners to see their statements. For instance, at IBS, legal persons can see bank statements only by sending official letters from their signatories and individuals can request their statements by using their fingerprints; tellers cannot see the statement if not requested by a customer.²¹ Salaam bank accounts can only be seen after user requests a statement and a PIN is sent to their registered phone numbers; the user provides the PIN to the teller, who then uses it to access the account. The tough security measures put in place by banks in the accessing of data appears to have pre-empted requests from AS.

Taxation

The Somali federal system is proving to be problematic for doing business; each FMS acts like it is a separate country -- it taxes banks and telecoms separately from the FGS and issues licensing fees. More confusing, there is an overlap in FGS and FMS central banks, with banks forced to comply with different regulations across the different regions.

The telecoms are not officially taxed by the FGS. The NCA is currently working on the taxing of telecoms; the regulation is in consultation. However, banks are taxed according to the income tax law, according to a bank executive. Banks that have reached profitability are required to pay profit taxes. Currently, it is only Dahabshiil and Salaam Bank that are profitable. Nevertheless banks are required to pay other fees such as licensing fees of \$1000 per year per branch and \$20,000 per year for the HQ.²²

Banks are required to have new permits for each new bank branch from the CBS and the local FMS; there are no bank branches in AS territory because the CBS

20 Interview with NCA official, December 2018; Interview with a Hormuud executive, March 2019.

21 Interview with an IBS executive, December 2018.

22 Interview with an IBS bank executive, December 2018.

does not issue permits except to the areas where there is government control. Nevertheless, NISA does not believe that AS taxes or even demands taxes from banks because banks hold other people's money and cannot be taxed according to Islamic law. Likewise, AS does not tax telecoms, as far as NISA is aware.²³

Taaj: Linking Hawala to mobile money and

The popularity of mobile money helped Taaj -- a money remittance company owned by Hormuud -- achieve astronomical growth in four years. Taaj was established in February 2013 across south and central Somalia. Owing to its connection to the EVC+ system, it has managed to take over 45% of the Hawala market in south and central Somalia.²⁴ Remittance of amounts less than \$300 are sent through EVC+ directly to the customer's number if the receiving name and EVC+ registration name match one another. If they don't, the money is sent as a Hawala and the person has to go and pick up the money from the office. The receiver has to provide a driving license, passport or govt I.D in order to take their money if it exceeds \$1000. If not, they have to provide a guarantor who has the aforementioned documents. IDs are required to send money. Remittances can be seen by any Taaj branch, but only receiving offices can pay them unless they change it themselves. The data on remittances are kept by the company for years; more recent transactions can be accessed by branch managers, and the older transactions by executives.

Interaction with the various polities

Different rules and ruling polities means complicated working conditions for businesses. The challenges of running a nationwide company in a nation ruled by rival administrations is illustrated by the problems telecoms companies faced in introducing mobile internet. Following the revelations of Edward Snowden about the NSA's snooping on internet-enabled devices, Al-Shabab banned mobile internet in 2013.

Hormuud, which was then the only mobile internet provider across south and central Somalia, switched off mobile internet in the regions but kept Mogadishu online. Al-Shabab directly ordered the company to cease providing mobile internet in Mogadishu as

well.²⁵ The telecoms brought back mobile WiFi in the capital by 2015, without consulting with Al-Shabab; nothing is illegal unless explicitly outlawed.

Interactions with FMS

Somalia's FMS offer big businesses the greatest challenges. Banks and telecoms are approached for 'contributions' towards projects by the leaders of all FMS, according to a bank executive. Refusing to pay them would result in harassment and the closure of branches.²⁶ The gravity of the matter is demonstrated by the fact that the executive said that the FMSs treat them worse than AS/ISS who have killed some employees of theirs. Because there is little rule of law in the FMSs, businesses have to directly deal with unaccountable local despots and 'contribute' to their pockets.

Interactions with Al-Shabab and Islamic

Nationlink and Olympic (now renamed SomTel) had the worst relations with all Islamist groups, including AS.²⁷ Similarly, Hormuud does not have good ties with AS: the company lost millions of dollars when the group banned mobile internet services. It is the position of NISA that telecoms companies do not cooperate with AS; for instance, in 2013, AS asked Hormuud to provide it EVC records of a former AS member; when Hormuud refused this, it was ordered to shut down 57 antennas in southern Somalia.²⁸ The same source claimed that major businesses use third hand tools in the form of other businessmen to lobby AS leaders to not hurt their businesses.

Nevertheless, individuals may share data with AS; there is no way to confirm whether this is happening. However, because telecoms log actions by its employees, it deters them from leaking data to AS. The data protection policies of the telecoms companies and banks limit what lower-level employees may share with AS. Bank data is almost impossible to fall into AS hands because of the stringent access procedures; AS is not known to have received bank statements.²⁹ However, as Hawala and some mobile money transactions data can be accessed by low-level employees in remote districts, it is possible and likely that individuals sympathetic to AS may access them and use the data to monitor

23 Interview with senior NISA official, December 2018.

24 Interview with Taaj executive, December 2018.

25 Interview with a Hormuud executive, December 2018.

26 Interview with a bank executive, January 2019.

27 Interview with a senior NISA official, December 2018.

28 Interview with a senior NISA official, December 2018.

29 Interview with a senior NISA official, December 2018.

potential targets -- for instance, by watching a known government mobile money account and following its transactions to pinpoint other officials or spies in AS territory. It can also be used by AS to monitor its own members for suspicious transactions.

NationLink: a case study in the effect of poor

Nationlink (NL) thrived in Mogadishu, managing to build good relationships across clan boundaries. However, its downfall started in 2006 as the Union of Islamic Courts gained power and the company failed to build a relationship with the group. The company considered UIC gains as a setback to its operations, as it believed that other companies were favoured by the Islamist groups. In 2009/10 NL was almost closed down due to AS pressures; the company was on the verge of closing down when AS left Mogadishu in 2011.

People left the existing infrastructure in the capital and companies were forced to build new infrastructure in the newly populated areas on the outskirts of the capital. The lost revenue from an emptied city was compounded by poor cooperation with armed groups, which in turn hurt their ability to quickly build new infrastructure in the newly populated areas. Things got so bad that AS killed seven NL employees and considered completely banning the company; other companies lobbied for AS to lift the ban, fearing it would put unwanted focus on them.³⁰

NationLink is still reeling from the war of 2009-11; it has lost most of its customers to Hormuud and SomTel. AS requires NL to ask for a prior permission in order to send a car to fix issues in a remote location, further undermining the company's ability to stay operational. AS banned an NL offline internet system that used SMS to connect to Twitter and Facebook in 2014/5.

Recommendations

1. Telecoms should make it harder for branch officers to access mobile money and call logs. They could do this by using the Salam Bank PIN system: a pin number is sent to the user to authenticate access to his data; only with the PIN may the data be seen.
2. Large money and unlimited mobile money accounts should be treated as any bank account. Individuals needing large transactions should prove purpose and origin of funds -- the telecoms companies should be covered in the AML/CFT law, and they should follow the regulations laid down by the FRC.
3. Following from the above, the telecoms companies

should be made part of the national compliance forum, which is currently made up of the banks, FRC, CBS, and FSV (financial service voluntary corps).

4. The FRC and the CBS both require better training and expertise to carry out their oversight responsibilities.
5. The FRC should define what exactly suspicious transactions are. The banks say it is unclear how many times someone has to come back and over how many days for the transactions to be considered suspicious.
7. Banks keep 70%-80% of their deposits and lend out only 10-30 per cent. This is because the banks are not forced to give out a particular amount of money to borrowers by the CBS. The CBS should do so in order to increase cash circulation and business opportunities.
8. There is no law on data protection; a data protection law should be passed in order to protect public and private data except from the authorities.
9. Likewise, there is no law requiring data retention; business institutions are collecting data mostly for business reasons. The government should therefore define how long data should be kept by banks and telecoms providers.
10. Banks and government regulators should be trained in new acts and regulations otherwise regulations without training becomes punishment.
11. Compliance training provided by the World Bank to the FRC should also be made available to the banks as they are the implementing stakeholders.
12. National ID is a priority that needs to be issued to control and monitor usage.
13. The Go AML system should be deployed in the FRC to assist it with better conducting its work.
14. Government should do more in security and make sure that it reaches everywhere in the country as banks have the most to lose from weak governance. Weak governance seems to be more dangerous than no governance.
15. In order to implement the telecoms law while maintaining telecoms service across Somalia, it is necessary for the government authority to expand to the areas currently occupied by Al-Shabab.
16. In order to encourage interconnectivity, antitrust laws need to be put into place to force banks to accept connection to all mobile money providers; the current system creates a situation whereby a few companies will corner the telecoms and banking sectors, an end situation which is not good for all concerned.