NetGuardians

CASE STUDY

CONSOLIDATED BANK GHANA

Consolidated Bank of Ghana turned to NetGuardians when it urgently needed a comprehensive, effective, easy-to-implement fraud-mitigation solution following its creation in August 2018 – as seven independent banks were merged into one.

Our partnership with NetGuardians delivers good benefits, especially for fraud in the digital space. You need smart solutions to assist in the fight against fraud to get the right alerts. We know we get this from NetGuardians. We also had some complex issues that it helped us identify that might have been difficult to do on our own.

Michael Amoah
Head of internal control
Consolidated Bank Ghana

The Requirement

Consolidated Bank of Ghana (CGB) has 114 branches and 119 ATMs across Ghana. It serves about 1 million active customers and processes approximately 300,000 transactions a day across its digital channels and between 30,000 and 40,000 in its branches.

When it was created by merging seven independent banks into one in August 2018, it was highly vulnerable to fraudsters. The different systems had significant concerns in their protection, each offering a potential exposure for fraudulent activities. As a result, there was an urgent need to put in place an effective fraud monitoring system to not only meet regulations, but also protect customers.

> When we started operating as one bank, we had no system/ tool for fraud monitoring and knew we faced a number of challenges especially across the administration activities on our core banking system.
>
> We needed an eye on what was going on, says Emmanuel Lalude, Head of Information Technology Control at the bank.

> There was an increasing concern over the possibility of fraud going undetected, especially due to the fact that these banks had different levels of exposure.
>
> We needed a system that could monitor user and customer behavior, among other things.
>
> **Michael Amoah, Head of Internal Control, CBG.**

The Solution

Six out of the seven Banks that formed CBG had previously been in discussions with NetGuardians. Five of those had been in early-stage talks and one had gone through a lengthy evaluation process during which it had vetted the NetGuardians software against that from other vendors.

> It wasn't too difficult to finalize the decision, says Lalude.

The individual Banks understood and liked NetGuardians' approach to fraud prevention. Rather than play a never-ending game of cat-and-mouse with the criminals, who are constantly reinventing their scams to avoid detection, the Swiss fraud-prevention specialist focuses on customer behavior to spot suspicious activity.

Its algorithms and machine-learning capabilities allow it to build up such detailed pictures of how a bank's customer behaves such that

it can spot an out-of-character transaction with exceptional accuracy. This approach not only protects the Bank from fraud, but also ensures customers are contacted only when the threat of a fraud is high, thereby ensuring a very good customer service. Furthermore, the system retains all audit trails, meaning historic data can be quickly accessed should any problem arise later.

Once the merged bank had completed a six-month project to consolidate its systems on to one core banking platform – T24 – it invited NetGuardians carry out the implementation of the NG|Screener - fraud monitoring solution.

Much of NetGuardians' functionality can be accessed via plug-and-play software which is compatible with many of the leading core banking platforms, including T24. It's usually a question of ensuring that the necessary data is being collected by turning on the relevant data fields that already exist within the core platform.

The NetGuardians software includes several AI risk models that monitor activities on the critical banking applications. Within a week of work starting, CBG could identify all user activities from a single console to spot out the irregular ones. Within three months, the full implementation, which includes comprehensive payment fraud monitoring across all channels, was completed with the help of First Vision Technologies (FVT), a local partner that works with NetGuardians.

The Benefits

The system is very handy, says Lalude.

The number of transactions we see in a day is huge.

Beforehand we had manual intervention to escalate any suspicious activity. Now it is automated. A central point gets an alert when there is a high-risk score and the alert sets out what the problem is. This makes it very easy to identify a password compromise, for example.

Violation alerts are generated real-time for every irregular activity speeding up the bank's response time to spot and prevent possible fraudulent activities.

The bank quickly benefited from its new fraud prevention software. For example, it is able to review audit trails kept by the system should any problem arise.

> We can get to the relevant information in minutes. Before, it would have been impossible as our audit trails were overwritten with the start of each new day, says Lalude.

Looking to the future, Lalude hopes to join NetGuardians' community program, NG|Club, which shares information about frauds and fraud prevention gathered from banks across the world. It really is a team effort.

Working with FVT, NetGuardians' local partner, the support NetGuardians gives CBG is in Lalude's words "superb."

> Dickman Adarkwah, CEO FVT, says: We are committed to offering excellent support to ensure CBG's ongoing success.

The solution offers visibility and control over the fraud landscape helping the bank to protect customer and stakeholder interests.

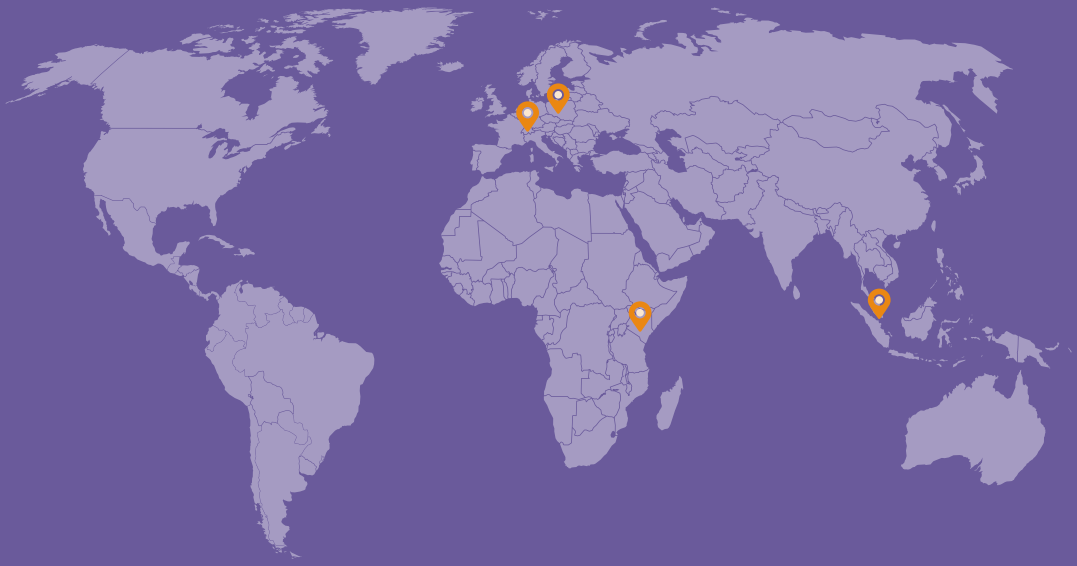
Contact us

NetGuardians Headquarters
Y-Parc – Avenue des Sciences 13
1400 Yverdon-les-Bains
Switzerland
+41 24 425 97 60

NetGuardians Africa
The Mirage Tower 1, 12th Floor
P.O. Box 574
00606 Sarit, Nairobi
+254 796 616 263

NetGuardians Asia
WeWork | NetGuardians
71, Robinson Rd, #14-01
Singapore 068895
+65 6224 0987

NetGuardians Eastern Europe
WeWork
Krucza 50, 00-025
Warsaw, Poland



RiskTech 100 2022

NetGuardians

www.netguardians.ch | info@netguardians.ch