Insights from Five Related U.S. Criminal Court Cases

International Criminal Organization Executed Multi-Layered Fraud Schemes; Stole From Hundreds of Victims, and Laundered Millions

By Denise Hutchings

VERAFIN
A STEP AHEAD

March 1, 2022

Insights from Five Related U.S. Criminal Court Cases

By Denise Hutchings

In September 2021, thirty-five defendants were indicted in the Eastern and Northern Districts of Texas in five related criminal cases [1] that involve the operations of an international criminal organization known as Black Axe. The main focus of this piece is to share some key insights into this criminal organization's operations which have been compiled from various court documents for these five specific cases.

The conspiracy existed to launder victim money to various overseas accounts, businesses, and individuals.

The excerpt below from one court document [2] provides a brief synopsis of the essence of this investigation.

In 2017, the FBI, along with other federal agencies, began investigating a long-term, ongoing international conspiracy. The conspiracy targeted ***more than 100 victims — including state governments, domestic and international businesses, and vulnerable individuals*** *—wherein the conspirators communicated using encrypted chats and utilized other sophisticated tools and techniques to fraudulently obtain substantial amounts of money. The conspirators' access to and use of electronics was key to defrauding their victims.*

Using such electronics, the ***conspirators employed schemes involving unemployment insurance fraud, investor fraud, business email compromise, and romance scams to obtain victim money****. The conspirators have been known to commit identity theft to further their fraudulent schemes.* ***The conspiracy existed to launder victim money to various overseas accounts, businesses, and individuals****. Upon receipt from a victim, victim money was deposited into a domestic bank account. The owner of such bank account then transferred the victim money to a different bank account, while retaining a portion of the deposited victim money as compensation.*

[FBI Special Agent – name redacted] testified ***this process repeated multiple times, utilizing various bank accounts, as a mode of concealing the stolen funds before the victim money reached its destination, which was usually in China or Nigeria****. So far, the FBI has identified over 700 bank accounts associated with the Conspiracy, many of which belong to legitimate or pseudo-legitimate businesses.* ***The estimated global loss amount attributable to the conspiracy thus far is approximately $17,000,000****.*

It is worth noting that multiple local, state and federal law enforcement agencies collaborated on this investigation. [3]

1 USA v. Ita, et al; USA v. Ohide; USA v. Animashaun, et al; USA v. Esezobor, et al; USA v. Alao

2 Order of Detention Pending Trial (USA v. Ita, et al – Jequita Batchelor)

3 Federal Bureau of Investigation's Dallas Field Office; Homeland Security Investigations; Internal Revenue Service-Criminal Investigation; Department of Labor-Office of Inspector General; U.S. Department of State's Diplomatic Security Service (DSS); U.S. Postal Inspection Service; U.S. Citizenship and Immigration Service; Allen Police Department; Denton Police Department; Dallas County Sheriff's Office; Texas Department of Public Safety; Texas Rangers; and U.S. Marshals

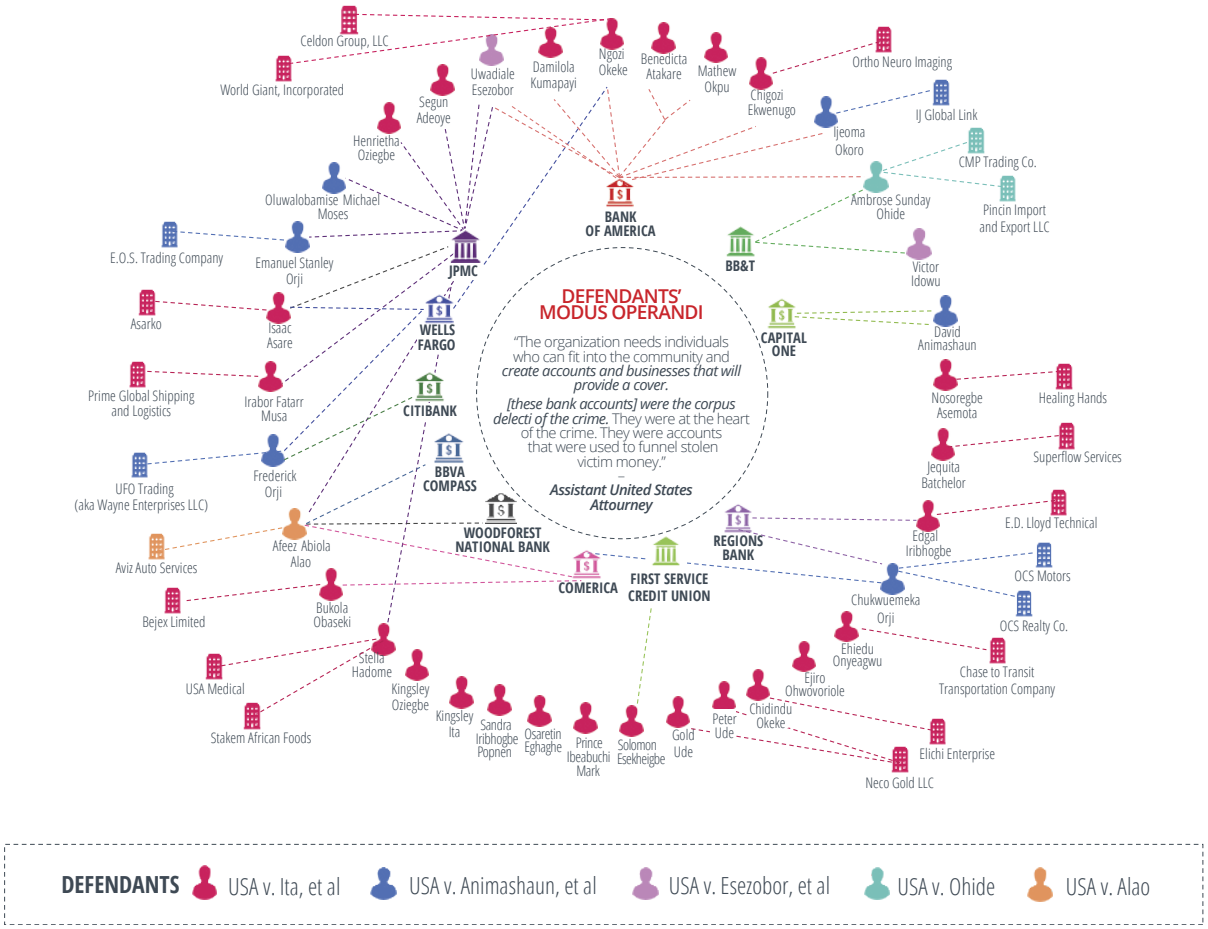
By Denise Hutchings

Voluminous Evidence Includes Records from Numerous Financial Institutions

The evidence illustrating the defendants' alleged criminal conduct in these cases is both voluminous and diverse. Law enforcement has collected records from numerous financial institutions showing accounts and transactions as one of several types of evidence against the defendants.

Figure 1 below is just a partial snapshot that depicts only a very small few of the numerous businesses and bank accounts associated with the defendants in this investigation.

Figure 1.



By Denise Hutchings

An Assistant United States Attorney (AUSA) stated in court :[4]

The way the indictment was alleged — of course, there's over $17 million in fraud that they've calculated, the IRS and FBI — at this point in this case; but the way we approached the indictment was to allege examples of each Defendant's involvement.

It would have been too long and too voluminous to attempt to allege every single transaction. So, we just chose examples of what the Defendants were involved in and put those specifically in the indictment. The proof at trial would include the broader picture.

Modus Operandi of the Criminal Organization

A police detective assigned to an FBI Task Force who testified at one of the detention hearings related to this investigation described the modus operandi of the criminal organization as follows: [5]

*Part of the MO of this operation is to **seek legitimate — or what appears to be legitimate employment to try to blend in below the radar**, if you will, to avoid detection.*

A few examples of this are illustrated below:

- Sandra Irbhogbe Popnen and Ehiedu Onyeagwu discussed opening bank accounts and using "fishing" as a cover for their fraudulent activity. During the conversation, Onyeagwu stated that once he opened the account, he would ***"explain to the bank right there that [I] am going to be doing a lot of foreign transaction so you people are aware, [I] am going to be doing some incoming and outgoing transfers."*** Onyeagwu then agreed to tell the bank that the transactions will be related to "fish." [6]
- Sandra Irbhogbe Popnen told Kingsley Oziegbe that they "just sent 50 thousand for fish." [7]
- Chigozi Ekwenugo is the owner of Ortho Neuro Imaging, an outpatient MRI center, and the sole signer on the company's bank account. Through Ortho Neuro Imaging, Ekwenugo received over $300,000 in victim money in 2020 from at least five different victims. These victims sent money directly to Ortho Neuro Imaging. A federal search warrant of co-defendant Sandra Iribhogbe's cloud storage revealed evidence that the victim money received by Ortho Neuro Imaging was subsequently wired internationally for payments not consistent with the business, for example "fish imports." [8]

Part of the MO of this operation is to seek legitimate — or what appears to be legitimate employment to try to blend in below the radar, if you will, to avoid detection.

4 Transcript of Proceedings, Detention Hearing, Southern District of Texas, September 27, 2021

5 Ibid.

6 Indictment, USA v. Ita, et al – Sandra Iribhogbe Popnen

7 Ibid.

8 Order of Detention Pending Trial – Chigozi Ekwenugo, Eastern District of Texas, October 19, 2021

Message Disseminated to the Membership of Black Axe

An AUSA noted that "the organization needs individuals who can fit into the community and create accounts and businesses that will provide a cover."[9] The following was a message disseminated to the membership of Black Axe:

As [a member] even if u must engage in some form of this illicit business (fraud) you must have other source of income by registering a business venture, even if it means a petty trade like selling of recharge cards in a small kiosk, selling cement, carwash, bars, eater etc to front with. Because when all these legal businesses are in place u can confidently speak up and defend urself when the need arises. (sic)

The evidence collected in the investigation confirms that this was not merely guidance; it described the defendants' modus operandi perfectly.

The AUSA stated that opening accounts that purport to be business accounts which are used to launder money through is at the heart of the scheme.[10] The AUSA made this statement in court:[11]

"They [these bank accounts] were the corpus delecti of the crime. They were at the heart of the crime. They were accounts that were used to funnel victims' stolen victim money."

"The AUSA stated that opening accounts that purport to be business accounts which are used to launder money through is at the heart of the scheme. They [these bank accounts] were the corpus delecti of the crime. They were accounts that were used to funnel victims' stolen victim money."

Black Axe Confraternity/Neo Black Movement

For the benefit of readers who may not be familiar with the sophistication of this criminal organization and the extent of their global criminal activity, I have provided some general background information below about Black Axe and their recent activity in various international jurisdictions before continuing with further details about the five aforementioned U.S. court cases on page 8.

A 2020 Analytical Report by Interpol[12] characterizes the Black Axe Confraternity as an Organized Crime Group (OCG) that has been active in cybercrime on the African continent as well as abroad, including in Canada, Italy and the U.S.

A 2018 Intelligence Report by cybersecurity firm CrowdStrike[13] provides a profile of the Black Axe Confraternity. The information below was published by CrowdStrike's Global Intelligence Team.[14]

9 Government's first amended consolidated response to defendants" motions to revoke detention orders

10 Transcript of Proceedings, Detention Hearing, Southern District of Texas, September 27, 2021

11 Transcript of Detention Hearing, Eastern District of Texas, September 28, 2021

12 Interpol Analytical Report: Online African Organized Crime from Surface to Dark Web, July 2020

13 CrowdStrike Intelligence Report: Nigerian Confraternities Emerge as Business Email Compromise Threat, March 2018

14 Ibid.

By Denise Hutchings

The Neo Black Movement (NBM) was founded in 1977 at the University of Benin, Nigeria. NBM claims that it is an officially registered organization in Nigeria, however it is widely considered to be one and the same as the Black Axe confraternity, and both have been banned by law.

Since its foundation, Black Axe has developed into a formidable criminal organization and has developed a hierarchical, inter-state organization while at the same time retaining cult-like tendencies.

Black Axe gangs are involved in a multitude of organized crime ventures such as running prostitution rings, human trafficking, narcotics trafficking, grand theft, money laundering, and email fraud/cybercrime. These activities primarily take place in Nigeria, and also are conducted by Black Axe members (a.k.a. Axemen) in Europe and North America.

Black Axe maintains a hierarchical command structure at the national level, and it also operates Black Axe "Zones" (also pyramidal in structure) in foreign locations.

A 2021 BBC News Investigative Report stated that operations by international law enforcement agencies indicate that Black Axe's scamming profits may run into the billions.[15]

The information below was published in the BBC reporting.[16]

For two years BBC Africa Eye investigated Black Axe, building a network of whistle-blowers, and uncovering several thousand documents leaked from the gang's private communications. The findings suggest that over the past decade, Black Axe has become one of the most far-reaching and dangerous organized crime groups in the world. The leaked documents show members communicating between Nigeria, the UK, Malaysia, the Gulf States, and a dozen other countries.

Emails detail elaborate and lucrative internet fraud. Messages plan global expansion. It was a mosaic of Black Axe criminal activity spanning four continents — Africa, Europe, Asia and North America.

Black Axe's global expansion has been carefully constructed. The correspondence shows Axemen dividing geographic areas into "zones," and designating local "heads."

The BBC reporting also stated that the U.S. Department of Justice has labelled the NBM a "criminal organization" and says it is "part of the Black Axe"; and Canadian authorities have said that the Black Axe and NBM "are the same."[17]

> *"The enterprise has local, national, and international leadership; a formal recruiting process; communication protocols; governing philosophies and documents; and operational meetings and plans."*

15 BBC News – Black Axe: Leaked documents shine spotlight on secretive Nigerian gang, December 13, 2021

16 BBC News – The ultra-violent cult that became a global mafia, December 13, 2021

17 BBC News – Black Axe: Leaked documents shine spotlight on secretive Nigerian gang, December 13, 2021

By Denise Hutchings

Various Leadership Positions of a Black Axe Zone Are Outlined in an October 2021 Indictment in the U.S. District of New Jersey

United States Secret Service (USSS) agents and their counterparts, the HAWKS (South African Police Service Directorate for Priority Crime Investigation), have been gathering evidence since 2018 of Black Axe's alleged involvement in business email compromise and romance scams.[18]

In October 2021, seven leaders of the Cape Town Black Axe Zone and an eighth man who conspired with a Black Axe leader, were charged with multiple federal crimes relating to internet scams they perpetrated from South Africa (SA).

The U.S. Department of Justice (U.S. DOJ) said that the suspects are charged with wire fraud conspiracy and money laundering conspiracy, spanning from 2011 to 2021.

U.S. DOJ said that the accused allegedly "used the bank accounts of victims and individuals with U.S.-based financial accounts to transfer the money to SA" and sometimes "convinced victims to open accounts in the U.S." that they would use themselves. After that, they would allegedly launder the money through businesses.

Conspirators worked to launder money derived from business email compromise schemes, romance scams and advance fee schemes. In addition to their aliases, the conspirators used business entities to conceal and disguise the illegal nature of the funds.

Black Axe has operated in various countries, including South Africa, and is organized into regional chapters known as "zones." Black Axe worldwide is governed by a National Council of Elders. Members of Black Axe are referred to as "Axemen" or "Ayes." [19]

The Cape Town Zone of Black Axe was formed around 2013.

Law enforcement sources said the Cape Town Zone was so important to Black Axe that its global leaders, based at its headquarters in Benin City, Nigeria, and in the US, UK and Italy, would travel to Cape Town for annual meetings.[20]

The Zone had various leadership positions, including the following: [21]

> *"The organization employed a variety of schemes, including romance scams, business email and investor schemes, and unemployment insurance fraud to obtain money."*

18 MSN South Africa – Crackdown on alleged internet scammer group Black Axe, October 2021

19 USA v. Osagiede et al, Superseding Indictment

20 MSN South Africa – Crackdown on alleged internet scammer group Black Axe, October 2021

21 USA v. Osagiede et al, Superseding Indictment

"Zonal Head" functioned as the Zone's chief executive officer and was responsible for coordinating and presiding over Zone meetings and supervising the Zone's activities. The Zonal Head prepared annual reports regarding the Zone's progress and sent those reports to Black Axe's worldwide leadership.

"Chief Ihaza" functioned as the Zone's treasurer and was responsible for keeping the Zone's financial records and for collecting dues, levies, and donations from members of the Zone.

"Chief Eye" functioned as a recording secretary and prepared and kept records of proceedings of Zone meetings, aided by the "Assistant Eye."

"Chief Butcher" functioned as the Zone's security officer and was responsible for disciplining members of the Zone, aided by "Assistant Butchers."

In addition to these leadership positions, the Zone was governed by a **Council of Elders, which was run by a Chairman.**

> *"The defendants used sophisticated means to execute and conceal their conduct, including "front" businesses, fake identities, multiple bank accounts, and insiders at financial institutions."*

Black Axe Activity in Italy, Ireland, Germany and Canada

Italy

In Italy, decades-old mafia laws are being revived to tackle the expansion of Black Axe, who are said to be overwhelming local crime networks.[22]

In April 2021, Italian police arrested 30 people suspected of belonging to the Nigerian Black Axe mafia gang that has been operating in many regions of the country. The suspects face almost 100 charges, including mafia association, drug and people trafficking, illegal immigration, prostitution and internet fraud.

The gang allegedly used cryptocurrency to carry out clandestine financial transactions on the dark web.[23] Police said most of the suspected crimes were committed on the internet, including using Bitcoins on the dark web to purchase the numbers of cloned credit cards, which were used for online shopping sprees.[24]

Several years earlier, a 2017 report by the Cambridge Centre for Applied Research in Human Trafficking (as cited in an Austrian Red Cross/ACCORD report[25]) noted that Black Axe had established itself in Palmero, Italy and was involved in drug dealing, prostitution and the fraudulent transfer of money between Europe and Nigeria.

22 BBC News – The ultra-violent cult that became a global mafia, December 13, 2021

23 BBC News – Black Axe mafia: Italian police arrest 30 Nigerian suspected gang members

24 Reuters – Italian police arrest 30 suspected Nigerian gang members, April 2021

25 Austrian Red Cross/Austrian Centre for Country of Origin & Asylum Research and Documentation (ACCORD) – Nigeria: COI Compilation on Human Trafficking, December 2017

Ireland – reference to laundering funds in Germany

In November 2021, two 'low-level' Cork-based operatives were jailed for their part in a pandemic unemployment payment (PUP) fraud masterminded by the head of Black Axe. [26]

They stole €183,000 but were working on a scheme to steal €1,000,000 and communicating via WhatsApp on how to launder that amount of stolen funds. The pair were in communication with someone who they referred to as "the Chairman" where they discussed laundering funds, partly via bank accounts located in Germany.

In one call, there is talk of how €30,000 of the proceeds of the Cork-based fraud was being laundered through accounts in Germany.

Canada

Arrests of Black Axe members by police in Toronto, Canada in 2015 revealed that the Black Axe Zone for Canada was heavily involved in wire fraud, money laundering, romance scams, and business email compromise (BEC). Police charged one of the individuals with the crime "money laundering for criminal organization" because they identified him as the bookkeeper for Black Axe's Canada Zone. [27]

The BBC Africa Eye Investigation cited previously reported that in 2017, Canadian authorities broke up a money laundering scheme linked to Black Axe. The BBC News story claimed that it was worth in excess of $5 billion.

> *Unlike many fraud schemes where ill-gotten funds are immediately cashed, spent on personal expenses, or laundered through domestic businesses, these defendants laundered these funds internationally, making it challenging to trace.*

Synopsis of Aforementioned Five Related 2021 Black Axe Prosecutions in the Court Districts of Eastern and Northern Texas

- *Criminal Organization that Runs with Structure and Purpose*
- *"Front" Businesses; Fake Identities; Multiple Bank Accounts; and Insiders at Financial Institutions*
- *Business Email and Investor Schemes; Romance Scams; and Unemployment Insurance Fraud*
- *Funds Laundered Internationally*

An Assistant United States Attorney wrote in a court document that "the nature and circumstances of the crime are uniquely aggravating and deviate from the vast majority of fraud cases." She further elaborated on this statement as follows. [28]

26 Irish Examiner – From Cork to Nigeria: Gang of cybercriminals caught out by their own technology, November 13, 2021

27 CrowdStrike Intelligence Report: Nigerian Confraternities Emerge as Business Email Compromise Threat, March 2018

28 Government's first amended consolidated response to defendants" motions to revoke detention orders

First, these defendants are part of a Nigerian criminal organization and/or have strong financial and criminal connections to the organization known as Black Axe. This international criminal organization has hundreds of members worldwide and operates under a philosophy of Pan-Africanism and militant action. Like other criminal organizations, such as drug cartels and terrorist cells, this one runs with structure and purpose. The enterprise has local, national, and international leadership; a formal recruiting process; communication protocols; governing philosophies and documents; and operational meetings and plans. In addition, like other criminal organizations, this group requires secrecy, demands loyalty, and uses violence.

Second, the number and type of victims here make the crimes here particularly egregious. The organization employed a variety of schemes, including romance scams, business email and investor schemes, and unemployment insurance fraud to obtain money. Moreover, the defendants used sophisticated means to execute and conceal their conduct, including "front" businesses, fake identities, multiple bank accounts, and insiders at financial institutions. The victims include individual people, businesses and companies, and government entities. Perhaps what is most unfortunate, though, are the scams targeting elderly victims, many of whom lost their life savings.

Third, the international scope of the offenses is staggering. Unlike many fraud schemes where ill-gotten funds are immediately cashed, spent on personal expenses, or laundered through domestic businesses, these defendants laundered these funds internationally, making it challenging to trace. Financial records and communications show how the defendants set up international businesses, including in Nigeria, China, and Hong Kong, that would receive wire transfers directly from victims or indirectly from domestic accounts controlled by the defendants.

At least 100 victims — including individuals, businesses, and government entities — sent money to the defendants and their co-conspirators. As a result of the fraudulent conduct, these victims lost at least $17 million.

“At least 100 victims — including individuals, businesses, and government entities — sent money to the defendants and their co-conspirators. As a result of the fraudulent conduct, these victims lost at least $17 million.”

Manner and Means of the Conspiracy

The following outlines the manner and means by which the defendants sought to accomplish the purpose of the conspiracy.[29] The defendants and their co-conspirators:

- communicated with each other by phone, WhatsApp text message, in-person meetings, and email regarding their fraudulent conduct
- used code words and dialects to disguise the true intentions and nature of their schemes

29 USA v. Ita, et al, Indictment

- employed a variety of deceptive schemes, including romance scams, business email compromises and investor fraud, and unemployment insurance fraud
- requested and coerced money from their victims using false identities and false representations
- received money from victims in various forms, including wire transfers, cash, and cashier's checks
- used hundreds of financial accounts, oftentimes in a business name or another individual's name, for the purpose of depositing, withdrawing, and transferring victim money
- forced unwilling individuals, including employees at financial institutions, to open accounts, create businesses, and deposit and withdraw money
- used virtual private networks (VPNs) and other similar tools to mask the locations from which they were conducting their fraudulent activity
- created and registered domestic and international businesses to legitimize their fraud
- shared business and residential addresses with each other to coordinate mailings and the receipt of victim funds
- used victim money for personal expenses
- sent victim money to bank accounts, co-conspirators, and businesses located in Africa and Asia (e.g. Hatford Resources Nigeria, Sedala Ventures, Temrex Nigeria Limited, Jedi Recycling, Foshan City Gaoming Sunnaise Plastics, Xiamen Heron Seafood, Kyokuy Company)
- after exchanging money in the United States, would engage in parallel transactions with foreign currency such as Nigerian Naira
- lied regarding their marriage and immigration status so that they could illegally stay in the United States to further their scheme
- caused wire transmissions that affected interstate and foreign commerce

> *The defendants not only coordinated how to exact money from their victims, but also how to disguise, disburse, and launder that money once they successfully defrauded their victims.*

Pervasive Exploitation of the Financial System

The financial institutions noted on Figure 1 (page 2) depict just some of the U.S.-based financial institutions at which conspirators held bank accounts. Various court documents reveal the far-reaching and diverse extent of this criminal organization's exploitation of the overall financial system.

By Denise Hutchings

Victim Bank Accounts at Numerous U.S.-based Financial Institutions

Victim money was stolen from bank accounts at numerous U.S.-based financial institutions including: USAA Federal Savings Bank; TD Bank; Charles Schwab; Merrill Lynch and Co. Inc.; Keybank National Association; Bank of New York Mellon; Bank of the Ozarks; Centennial Bank; Community Resource Credit Union; Bank of America; U.S. Bank; Wells Fargo; and JPMorgan Chase.

"This criminal enterprise, is very well-versed in the art of money laundering. They're very, very good, and have for a long time been very successful at avoiding the detection of law enforcement."

A Small Sample of the Numerous and Tragic Victim Stories

- A woman over 80-years-old was told by a conspirator that a child was being held hostage and that if she refused to transfer funds, the child would be killed. That victim transferred over $200,000 to the conspiracy.[30]
- An 82 year old woman who was being victimized up until the day the FBI met with her still didn't believe the FBI after they left trying to prove to her that she was being victimized.[31]
- A Navy veteran mortgaged his home and gave that money to his predator. He lost his home and over $200,000 [32]
- A 73-year-old widow lost more than $500,000 [33]
- A 71-year-old woman lost approximately $700,000 [34]

International Financial Institutions and Conspirator Bank Accounts

Victim money was sent by the conspirators to financial institutions in several countries including China, Thailand, Japan, and Nigeria.

Examples of foreign financial institutions noted in various court document include Fidelity Bank, Zenith Bank, United Bank of Africa, Lagos Bank and GT Bank.

Use of Insiders at Financial Institutions

One defendant, Chidindu Okeke, allegedly recruited accomplices, including bank employees.

- Okeke recruited a Wells Fargo employee to be an accomplice in the scheme. A Magistrate Judge noted that *"Defendant told the Wells Fargo employee his name was Steve and he began to sweet-talk and romance her. Defendant convinced her to open accounts in her name and he directed money to be transferred into those accounts."*[35]

30 Order of Detention Pending Trial, Peter Ude, October 7, 2021
31 Transcript of Detention Hearing, Eastern District of Texas, September 28, 2021
32 Ibid.
33 Pretrial Detention Order, Ngozi Okeke, October 7, 2021
34 Transcript of Arraignment and Detention Hearing, Eastern District of Texas, October 20, 2021
35 Order of Detention Pending Trial – Chidindu Okeke, Eastern District of Texas, December 6, 2021

- Okeke asked a bank employee to register a business name, open multiple bank accounts, and help move money through those accounts. When discussing a specific BBVA bank account, Okeke instructed the employee to withdraw "9800 or 9900" and not do "10k again" in order to avoid detection. [36]

Aliases and Fake Passports to Open Bank Accounts

Co-conspirators used fake names on forged passports to open bank accounts in the United States to receive victim funds. An example of this is noted below. [37]

"Daniel Christopher" and *"Lawrence Moses"* are aliases used by Uwadiale Esezobor on fake and forged Nigerian passports.

- Uwadiale Esezobor used the fake Nigerian passport in the name "Daniel Christopher" to open an account at JPMorgan Chase Bank and an account at Bank of America.
- Esezobor used the fake Nigerian passport in the name "Lawrence Moses" to open an account at JPMorgan Chase Bank and an account at Bank of America.

Money Bounced Rapidly Through Various and Multiple Accounts

The defendants not only coordinated how to exact money from their victims, but also how to disguise, disburse, and launder that money once they successfully defrauded their victims.

An FBI Task Force Officer who testified at one of the detention hearings stated:

This criminal enterprise, is very well-versed in the art of money laundering. They're very, very good, and have for a long time been very successful at avoiding the detection of law enforcement.

One of the tactics that they use — since they know that we can't identify the person behind the keyboard, they know that we're going to follow the money — one of the tactics that they employ is to move that money out of the account as quickly as possible and move it in a variety of ways. The faster it moves, the more often it moves, the more difficult it is for law enforcement to trace it. [38]

When a victim is defrauded, they're usually instructed to send or wire that money to an account. And then, once it hits that account, pretty quickly it begins to move to other accounts. Then, it just gets bounced from account to account to account; and then, ultimately, it ends up, typically, in an international account.

> *One of the tactics that they use — since they know that we can't identify the person behind the keyboard, they know that we're going to follow the money — one of the tactics that they employ is to move that money out of the account as quickly as possible and move it in a variety of ways.*

36 USA v. Ita, et al – Chidindu Okeke, Indictment

37 USA v. Esezobor, et al – Uwadiale Esezobor, Indictment, September 15, 2021

38 Transcript of Proceedings, Detention Hearing, Northern District of Texas, October 1, 2021

By Denise Hutchings

Law enforcement agencies, the Govern — the IRS, FBI, we have the ability to track funds through accounts; but when it begins to bounce rapidly, especially through various and multiple accounts, it makes it much more difficult to track those funds. ***So, it's a tactic that's commonly used to kind of conceal, avoid detection...***[39]

A Grand Central Station for Money Exchanges Related to Fraud

An Assistant United States Attorney characterized the activities of two of the defendants [Sandra Irighogbe Popnen and Edgal Irighogbe] as "a grand central station for money exchanges related to fraud" in some of the questions she posed to an FBI Special Agent at a detention hearing:[40]

Question: *And were they constantly doing financial transactions? Cash was coming, being sent to them by mail, they were doing banking transactions, and were in touch with multiple other individuals; is that right?*

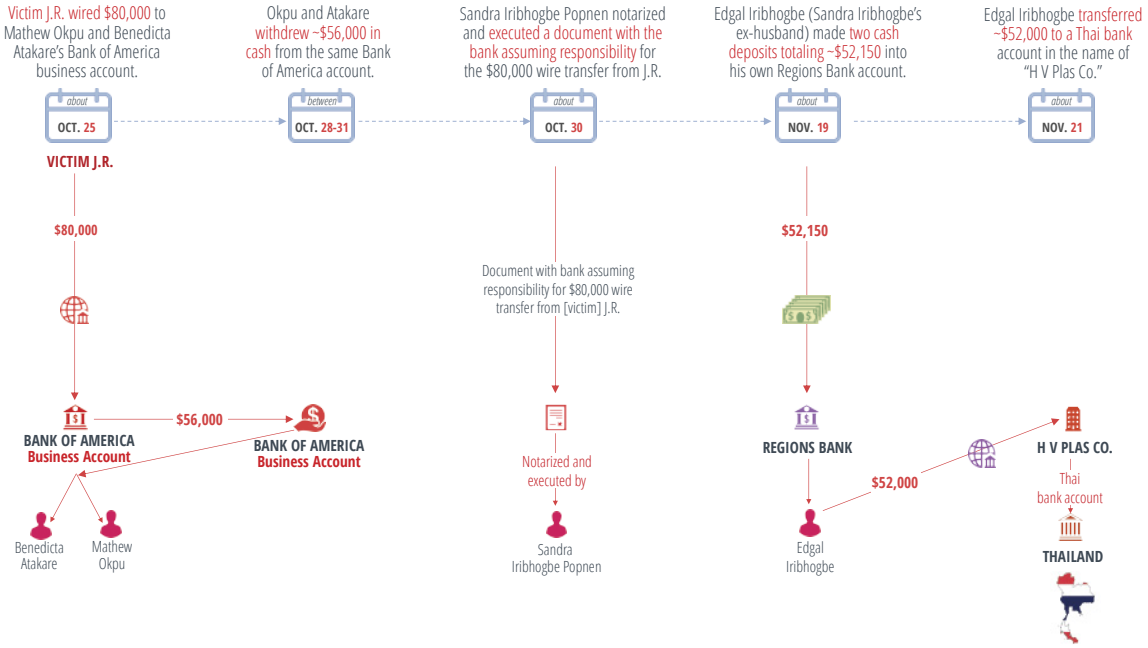
Answer: *Yes, ma'am.*

Question*: And was it determined that essentially they were somewhat of a grand central station for money exchanges related to fraud in the case?*

Answer: *Yes, ma'am, you could say that.*

Figure 2 below is one example of money movement involving these two defendants.

Figure 2.



39 Transcript of Proceedings, Detention Hearing, Southern District of Texas, September 27, 2021

40 Transcript of Arraignment and Detention Hearing, Eastern District of Texas, October 20, 2021

Money Moved via Wires; Checks; Cashier's Checks; Cash; Prepaid Cards; P2P Transactions; and, Cryptocurrency

The AUSA also posed questions about the movement of stolen victim money to the FBI Special Agent at the detention hearing:

Question: *Okay, explain to us how the money would be moved from account to account and why?*

Answer: *Well, why would be to conceal where it was coming from and to move it so that it was harder to detect from law enforcement.*

It would be moved via checks. Multiple checks would be sent. Sometimes cash was sent by victims.

Additionally, you have peer-to-peer type applications where the money could be sent. ***Zelle would be a popular one that we saw during the course of this investigation.***

In addition to the payment methods noted above, various court documents refer to: wires; Western Union transfers[41]; MoneyGram[42]; Coinbase[43]; and Green Dot and other prepaid cards.[44]

Sample Details re: the Financial Activities of Various Co-conspirators

- [FBI Special Agent – name redacted] testified that, based upon his investigation, he believes Irabor Fatarr Musa, an alleged leader in the conspiracy, has over 20 bank accounts, both domestic and foreign, including accounts located in Nigeria.[45]
- [FBI Task Force Officer – name redacted] testified that Chukwuemeka Orji was a signer on 24 different bank accounts between 2014 and 2019.[46]
- During a search of Frederick Orji's residence, investigators located approximately 250 stored-value cards or Green Dot cards in his possession.[47]
- During a search of OCS Motors, a business owned by Chukwuemeka Orji, an investigator located a bag that was concealed inside a printer. When you reached in and up and removed the drawer, there was a bag that contained a passport for someone else, a credit card skimmer, a chip reader and a plethora of prepaid cards and blank IDs.[48]

> *The faster it [the money] moves, the more often it moves, the more difficult it is for law enforcement to trace it.*

41 Order of Detention Pending Trial – Bukola Obaseki, October 19, 2021
42 Transcript of Detention Hearing, Emanuel Stanley Orji, October 29, 2021
43 Order of Detention Pending Trial – Kingsley Ita, October 7, 2021
44 Transcript of Proceedings, Detention Hearing, Northern District of Texas, October 1, 2021
45 Order of Detention Pending Trial – Irabor Fatarr Musa, October 15, 2021
46 Transcript of Proceedings, Detention Hearing, Northern District of Texas, October 1, 2021
47 Ibid.
48 Ibid.

- [FBI Task Force Officer – name redacted] testified that when investigators executed a search warrant at the home of David Animashaun (a.k.a. David Benson; a.k.a. David Brown), they located a notepad with multiple pages of personal identifying information (PII) which appeared to potentially involve Chinese citizens and contained their FICO scores.[49] The AUSA who questioned the FBI Task Force Officer stated *"that [PII with Chinese names, FICO scores, amounts next to them] is part and parcel of what the schemes, whether they're romance or unemployment fraud or business email compromise, need to perpetrate. They need the PII."*

Cryptocurrency

The Cape Town Zone Black Axe Prosecutions in the US District of New Jersey in October 2021, revealed that co-conspirators in that case have used cryptocurrency exchanges to launder money obtained by business email compromise frauds.[50]

The co-conspirators convinced romance scam victims to open accounts at cryptocurrency exchanges to conduct cryptocurrency transactions and to permit the co-conspirators to conduct cryptocurrency transactions for the co-conspirators' benefit, including cryptocurrency transactions that derived from business email compromises.[51]

Ongoing Investigation – More Subjects Anticipated to be Uncovered

An Assistant United States Attorney has noted that:

This investigation is ongoing. Not every defendant in this case has been located and arrested, and law enforcement anticipates that more subjects and victims will be uncovered as it processes new evidence.[52]

Conclusion

The five related U.S. criminal court cases reviewed in this piece certainly lend credence to the claim that Black Axe has indeed built a powerful international network.

This investigation is ongoing. Not every defendant in this case has been located and arrested, and law enforcement anticipates that more subjects and victims will be uncovered as it processes new evidence.

49 Ibid.

50 U.S. Attorney's Office, District of New Jersey, Press Release, October 19, 2021

51 USA v. Toritseju Gabriel Otubu – Indictment, September 20, 2021

52 Government's first amended consolidated response to defendants" motions to revoke detention orders

About Verafin

Verafin is the industry leader in enterprise Financial Crime Management solutions, providing a cloud-based, secure software platform for Fraud Detection and Management, BSA/AML Compliance and Management, High-Risk Customer Management and Information Sharing. 3500 banks and credit unions use Verafin to effectively fight financial crime and comply with regulations. Leveraging its unique big data intelligence, visual storytelling and collaborative investigation capabilities, Verafin significantly reduces false positive alerts, delivers context-rich insights and streamlines the daunting BSA/AML compliance processes that financial institutions face today.

Verafin is the exclusive provider for Texas Bankers Association, Western Bankers Association, and CUNA Strategic Services, with industry endorsements in 48 U.S. states.

Learn more

For more information on this topic, or how Verafin can help your institution stay a step ahead of financial crime, call 866.781.8433.

To access Verafin's archive of webinars, white papers, success stories and other materials focusing on BSA/AML compliance and fraud detection topics relevant to financial institutions across the country, check out our online Resource Center at **www.verafin.com**.