

United States v. Ogiekpolor

How a Georgia man who laundered more than \$9.5 million in scam proceeds received 25 years in federal prison

Court: U.S. District Court, Northern District of Georgia (Atlanta)

Investigated by: FBI Atlanta Field Office

Sentenced: October 3, 2022



Defendant	Elvis Eghosa Ogiekpolor, 46, of Norcross, Georgia
Convictions	1 count of conspiracy to commit money laundering; 15 counts of money laundering
Amount laundered	More than \$9.5 million
Sentence	25 years in federal prison, then 3 years of supervised release
Restitution	To be set at a later hearing
Judge	U.S. District Judge William M. Ray II

Background

Money laundering is the process of making criminal proceeds look legitimate so they can be spent without drawing attention. It usually happens in three stages: **placement** (getting the dirty money into the financial system), **layering** (moving it through enough accounts and transactions to hide where it came from) and **integration** (using it as if it were clean). The Ogiekpolor case is a textbook example of all three, and of how seriously federal courts treat the people who run the laundering side of large online fraud networks.

Between about October 2018 and August 2020, Ogiekpolor ran the financial machinery for an international network of online fraudsters. The fraudsters found the victims; his job was to receive the stolen money, hide its trail and send it on. In announcing the sentence, U.S. Attorney Ryan Buchanan described him and his co-conspirators as "part of a broader international network of online fraudsters."

How the scheme worked

Ogiekpolor recruited and directed at least eight "money mules." Following his instructions, they registered about a dozen sham companies and opened at least 50 business bank accounts in those companies' names. To a bank, the accounts looked like ordinary small businesses. In reality they existed only to receive fraud proceeds.

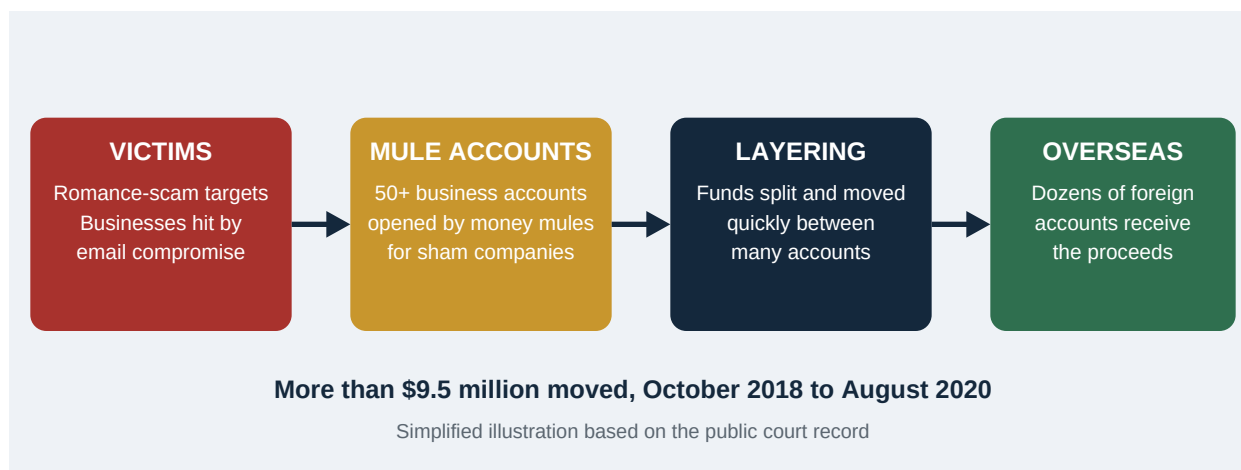


Figure 1. The path of the money, from victims to overseas accounts.

Money flowed in from two kinds of scams. In **business email compromise**, criminals impersonated suppliers or executives and tricked companies into wiring payments to the wrong account. In **romance scams**, fraudsters built fake dating profiles, spent months convincing victims they were in a relationship, then invented an emergency that required a large sum of money. Once funds landed in a mule account they were quickly split up and moved through other accounts, including dozens overseas, before victims or banks could react.

The victims

Many romance-scam victims were older people with significant savings, often retired widows and widowers. Thirteen of them testified at trial. One woman sent nearly \$70,000 to a man she met on eHarmony and never met in person. Beyond the financial loss, victims described lasting shame, isolation and damaged trust, which is one reason courts treat these cases so severely.

Investigation and trial

The FBI's Atlanta field office investigated the case, tracing deposits from victims through the mule accounts and on to their destinations. A federal grand jury indicted Ogiekpolor in February 2022. He went to trial, and six of the money mules he had directed testified against him. On May 31, 2022, after an eight-day trial, the jury convicted him on all 16 counts. Five of his co-conspirators had already been sentenced before him.

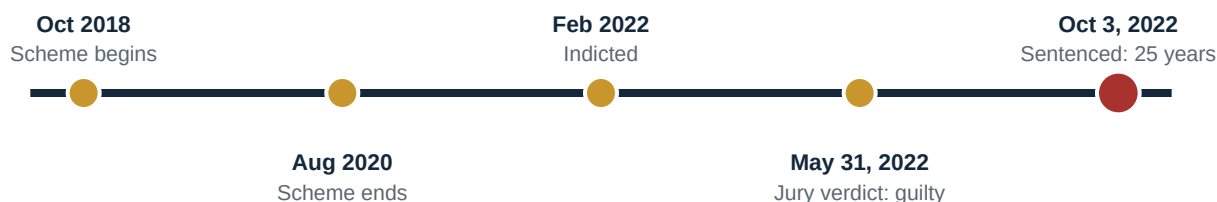


Figure 2. Key dates in the case.

Why 25 years?

Each federal money laundering count carries a maximum of 20 years, so a 25-year sentence shows the court treated this as an especially serious case. Several factors push federal sentences upward: the very large amount of money involved, the number of victims and how vulnerable they were, the defendant's role as an organizer who directed others, and the sophisticated use of shell companies and foreign accounts. Going to trial also meant he received no reduction for accepting responsibility. On top of prison time, he faces three years of supervised release and a restitution order to repay victims.



FBI Atlanta Special Agent in Charge Keri Farley said the sentence would hopefully give victims some comfort, while acknowledging that nothing can make them whole again, and stressed that the FBI treats these cyber-enabled crimes as a top priority.

Lessons and warning signs

- Never send money, gift cards or cryptocurrency to someone you have only met online, however long you have been talking.
- Confirm any change to a supplier's bank details by phone, using a number you already have.
- Be wary of job offers to "receive and forward payments." That is money-mule recruitment, and mules can be prosecuted too.
- Report fraud quickly. In the U.S., use the FBI's Internet Crime Complaint Center (ic3.gov). In Canada, contact the Canadian Anti-Fraud Centre.

Sources: U.S. Attorney's Office, Northern District of Georgia press release (October 2022); Associated Press / WSB-TV (October 4, 2022); The Record; The Hacker News; AML Intelligence. Figures are simplified illustrations of the public record.