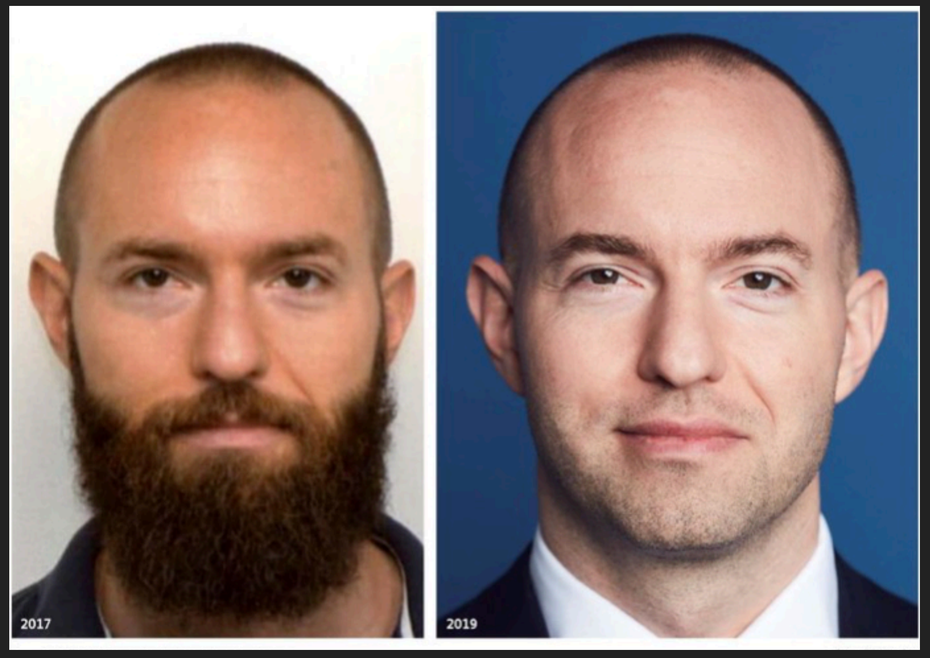
ANJISHNU BANDYOPADHYAY
SCIENCE MEETS BUSINESS
BCGS
19.04.2024

# CATCHING FINANCIAL CRIME WITH DATA

# FINANCIAL CRIME: HOW HEINOUS IT IS?

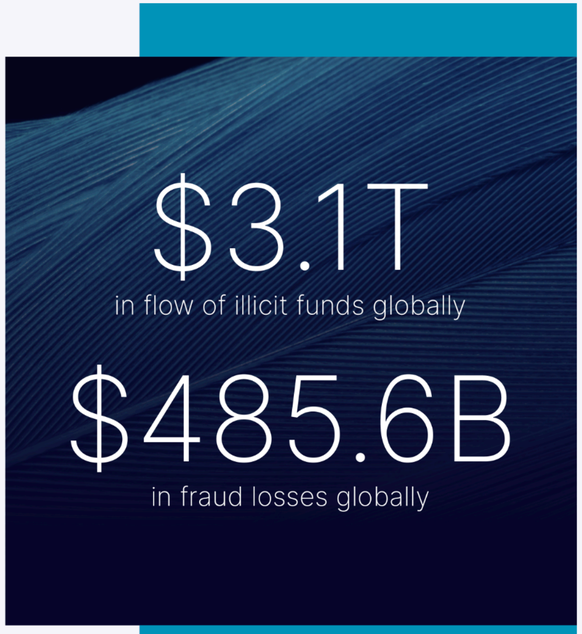
- Walter made 80 million, Marsalek frauded Wirecard of 2 billion




## The Global Scale of Financial Crime

In 2023, an estimated $3.1T in illicit funds flowed through the global financial system. Money laundering accounted for trillions of dollars funding a range of destructive crimes, including an estimated $346.7B in human trafficking and $782.9B in drug trafficking activity, as well as $11.5B in terrorist financing.

In 2023, fraud scams and bank fraud schemes totaled $485.6B in projected losses globally.




Source: Nasdaq report

# MONEY LAUNDERING

## PLACEMENT

Illicit funds are initially introduced into the financial system through deposits or purchases.

## LAYERING

Funds' origin is obscured through complex transactions and transfers across accounts.

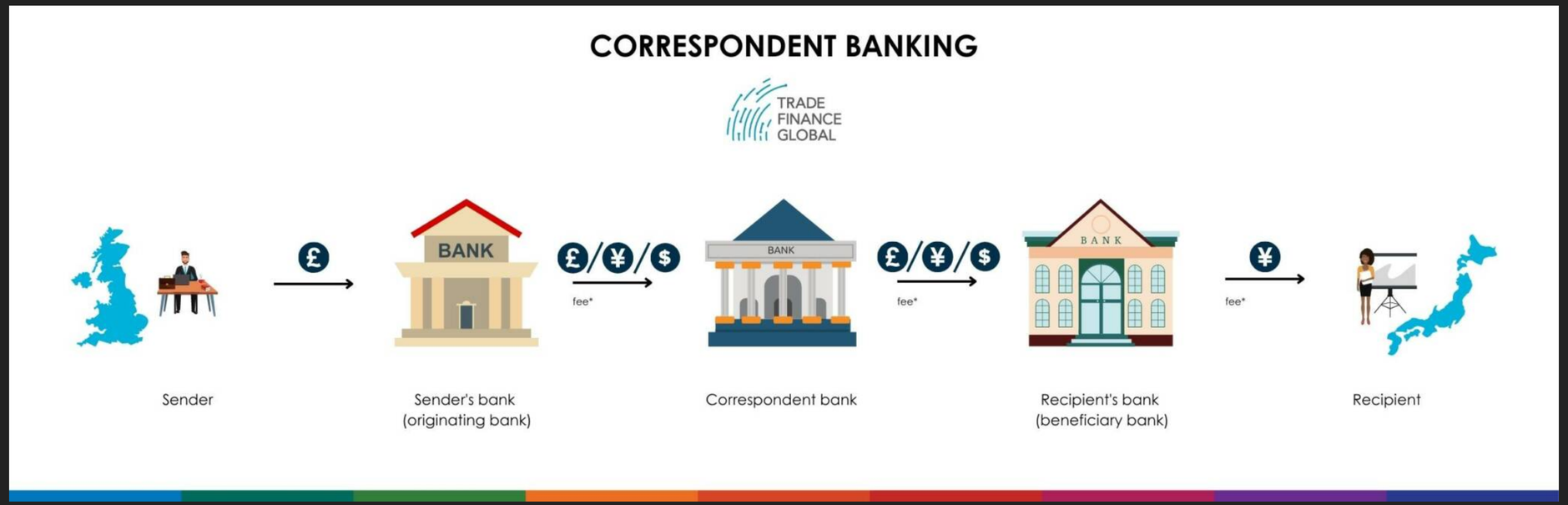
## INTEGRATION

'Cleaned' money is re-entered into the economy as legitimate, through investments or asset purchases.

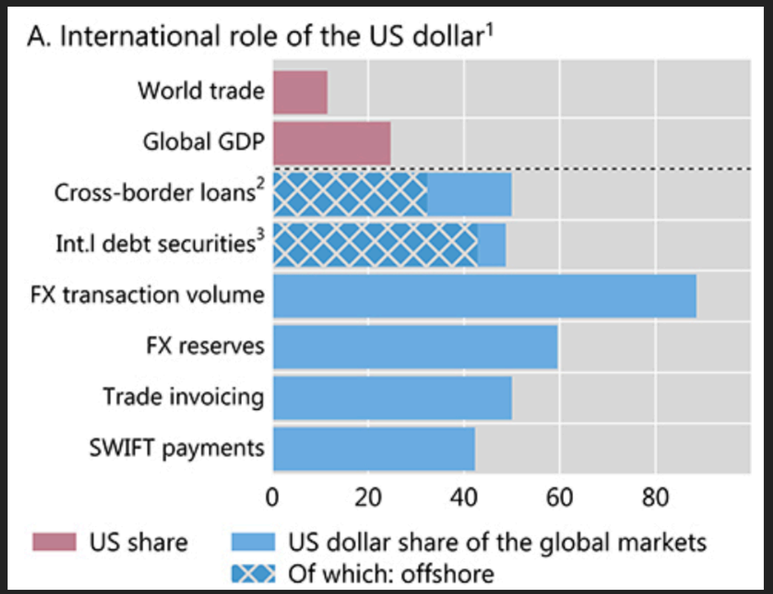
# ANTI-MONEY LAUNDERING (AML)

- How to do AML in the world of data-deluge and security and privacy?
  - Follow the money
  - Understand the letter of the law, because the spirit has been taken away long back.
  - Layering and integration are the steps that ate hardest to detect.
  - Develop new privacy enhancing AML technologies that can catch the bad apple.

# HOW THE MONEY FLOWS?



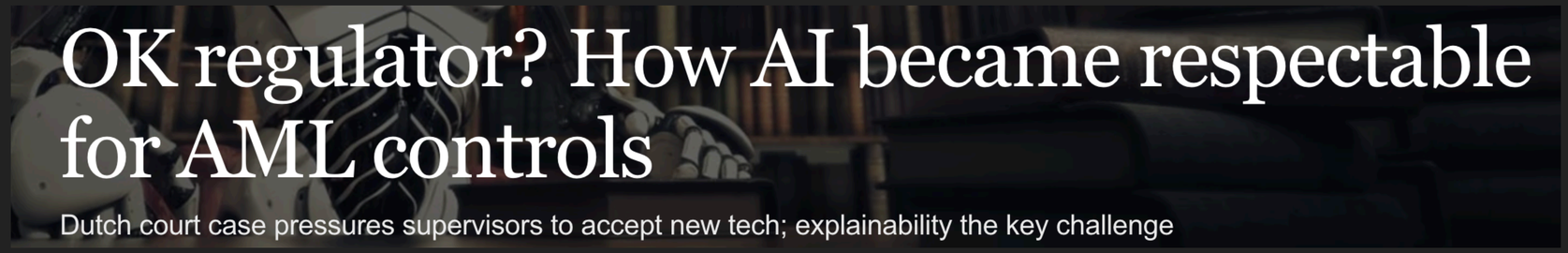

- Correspondent banking is the main way cross-border payments happen.
- The lion share of correspondent banking happens in US dollar.



# RISK TYPOLOGIES

- Financial Action Task Force recommends a risk-based approach to combat money laundering.
- FATF has a set of recommendations that banks and countries need to follow.
- For each transaction, we can measure risk typologies.
- Round amount payments
- Smurfing : Dividing large amount of transactions into small amount.
- Structuring : Payments just under threshold that would warrant scrutiny.
- Absence of payment transparency

# MACHINE LEARNING IN AML




- Anti-money laundering is an unsupervised machine learning problem. The true labels are not known.
- Anomaly detection is performed to detect suspicious transactions.
- Each transaction is a data point where risk typologies are input features to the model.
- Models like Isolation Forest, Autoencoders are used to build transaction monitoring systems.

# LARGE LANGUAGE MODELS FOR AML

- As with other fields LLMs also have use in AML.
- Perfect tool to extract and summarise risk typologies for various financial institutions at scale.
- Simple code takes Deutsche Bank annual report and answers various questions that are indicative of the risk.
- But have to be careful about hallucinations.
- Sentiment analysis of external news for financial institutions can be used

```
from langchain.chat_models import ChatOpenAI

llm = ChatOpenAI(model_name="gpt-3.5-turbo", temperature=0)

from langchain.schema.runnable import RunnablePassthrough

from langchain.prompts import PromptTemplate

template = """Use the following pieces of context to answer the question at the end.
If you don't know the answer, just say that you don't know, don't try to make up an answer.
{context}
Question: {question}
Helpful Answer:"""
rag_prompt_custom = PromptTemplate.from_template(template)

rag_chain = (
    {"context": retriever_from_llm, "question": RunnablePassthrough()} | rag_prompt_custom | llm
)

rag_chain.invoke("Does this report provide any evidence of presence of anti money laundering measures and policies? \
Please cite the page numbers you used to answer your questions")
```

```
INFO:langchain.retrievers.multi_query:Generated queries: ['1. Are there any indications in this report that suggest the implementation of anti-money laun
AIMessage(content="Yes, the report provides evidence of the presence of anti-money laundering measures and policies. This is evident from the sections
discussing the bank's anti-money laundering (AML) and know-your-client (KYC) processes, regulatory reviews, investigations, enforcement actions, and orde
related to preventing money laundering and terrorist financing. Specifically, pages 51, 82, and 411 provide information on the bank's efforts to enhance
internal controls, comply with regulatory requirements, and adopt appropriate safeguards to prevent financial crime.", response_metadata={'token_usage':
<OpenAIObject at 0x7b1c34f55940> JSON: {
  "prompt_tokens": 5417,
  "completion_tokens": 100,
  "total_tokens": 5517
}, 'model_name': 'gpt-3.5-turbo', 'system_fingerprint': 'fp_d9767fc5b9', 'finish_reason': 'stop', 'logprobs': None}, id='run-696a948d-6438-4265-8192-
b7f4b7f86c4f-0')
```

# ANTI-FRAUD AND MACHINE LEARNING

- In money laundering, the customers are mostly the perpetrators.
- In bank fraud, customers are the victims e.g. phishing fraud, scam fraud, blackmail fraud etc.
- Bank Fraud is a supervised machine learning problem. The true positives are present.
- Building risk typologies and finding their relation with the target variable, presence of fraud.
- Currently, I work for a Buy Now Pay Later company where fraud becomes a semi-supervised problem.
- Historical true positives are present, real time ones are not.

# COMPANIES LEADING THE REGTECH GAME WITH AI


A few companies from

https://fintech.global/regtech100/