



# Wannabe Senior Data Analyst @Verification Team

Take-home test

Csaba Elekes  
csabi.elekes@gmail.com



# Look for money laundering!

Goal of the project:

- By looking at a set of transactions find risky customers who might be trying to launder money
- Provide suggestions how to treat them



# Aspects of risk assessment

## First-time users -- identity

- Basic identification
- Check blacklists
- Amount limits

## Regular users -- behaviour

- Same as first-time transfers
- Too frequent attempts
- Unusual amounts
- Chains, loops, circles
- Non-invoice transactions from business account



# First time users - Basic identification

Ask basic information from users according to legislation ->

- Pictures of ID cards, passports
- Electronic identification if available

Treatment: part of sign-up process



# First time users - Blacklists

There are national and international lists of this kind

- User is on a blacklist
- Recipient of the transfer is on a blacklist
- Target country is problematic (e.g. Iran, Iraq, Afghanistan, Cuba)
  - Data set did not contain any transfers to and from these countries
  - I assume TransferWise's service is not available there

Treatment: go through the official channels using the info the customers provided



# First time users - Amount limits

Below certain amount (and frequency) the transfer doesn't pose a high risk of money laundering

- More relaxed rules

Above certain amount (e.g. \$1000) users can be asked for extra documents

- The UI + email can inform users that the transfer will be blocked until the documents are provided and checked
- Customer support may try to contact users who haven't taken an action
- Contacting CS before a large transfer might speed up the approval process



# First time users - Amount limits

Example user\_ids:

Never succeeded:

- 1a8ebb56a246a22b8dc164049c703e92
- 77fc14c6ba9a8046df80a6f1b85f87ab

Solved the issue later:

- 6008779d978132785979f29361c18bbe
- 6fab464b57a0b0fbe2d09d345fa32d4f



# Regular users - Too frequent attempts

Some users start several attempts within minutes from each other

- Most of the transfers never go through
  - Majority is cancelled before payment made
- 
- Business customers: ask for invoice, check if the company is legit
  - Personal customers: check transfer reference, payment method, recipient details in public registers, government databases





# Regular users - Too frequent attempts

Some users start several attempts within minutes from each other

- Most of the transfers never go through

Example user\_ids:

- 39ded89a9e1d1a7ee64742c701657716-> a lot of transfers, all of them cancelled before sending the money
- 8917c69f0a728519439d93ba9b49005a-> some kind of test account
- b78c8ce3f52611c3df21da6b9effe911-> may attempts on the first day, all failed
- d6fb6f9d8ca89d20d9db824b845159d0-> tons of self-transfers



# Regular users - Unusual transfers

## Too high amounts

- Top 1% of the amounts transferred in each currency is worth looking into -> manual checks from TW staff
- Contact customer, ask for extra proof (e.g. papers about house inherited and sold)

## Unusual activity of a returning user

- Might indicate cyber fraud, hacked account
- Regular transfers of low amounts, then one is much larger
  - d966e072fab4f783c66d30fa2ed4a723
- New recipient in new country
- Email + phone notification, delay transfer to give time for customer to notice it.



# Regular users - Chains, loops, circles

Money laundering and cheating with taxes can be an organised crime:

- Companies invoice each other in a chain or circle, and claim taxes back
- The first one doesn't pay taxes, but the rest receives refunds
- Cooperate with tax authorities

Due to the fact that the data is sampled it was unlikely to find these. The longest chain of transfers was of length 3 and looked legit.



# Regular users - Business accounts

Usual activity on the business accounts:

- Invoices
- Self-transfers
- Rent
- Freelance

But might be suspicious:

- Family
- Blank
- Other/unknown



# Code

[Notebooks on Github](#)