New Account Fraud

Manan Arora
Urvin Soneta
Neha Gupta
Shubham Saboo
Balbir Singh

5th December 2019

—

GCLS IV: Fin Tech

—

Gaurav Sharma

Problem Statement

XYZ Ltd. is a successful credit card company with more than 300K customers in the country. While it has very good credit and transaction fraud solutions, it is seeing a large increase in new accounts fraud (Fraudsters using personal information of other people to apply for credit card and then default on the payments).
The new account fraud applications look like any other normal application and does not seem to show significant difference on normal credit risk variables from Credit Bureau.
Ajay, who is the Chief Risk Officer for the company, is wondering how to reduce these new accounts fraud cases. He needs to find answers to the following questions:

- What are the data sources should he explore to be able to address the issue of identifying new accounts fraud applications?
- What are the top 5 variables ideas from each data source that he can use for this purpose?

Data Sources:

Behavioural Biometrics Data

It recognizes criminal behaviour by differentiating those behaviours from those of normal users. Behavioural biometrics offers a distinct advantage over other methods of personal security because it's a passive means of identification that does not require any time or technical know-how from users. The Behavioural biometrics data include keystroke dynamics, gait analysis, voice identification, mouse use characteristics, signature analysis and cognitive biometrics. It measures everything from how the user holds the phone or how they swipe the screen, to which keyboard or gestural shortcuts they use in order to determine user's identity on subsequent interactions.

- **Application fluency** — Fraudsters repeatedly using compromised or synthetic identities demonstrate a high level of familiarity with the new account opening process. The application fluency variable will map inconsistent behaviour patterns in the application flow to differentiate between human and non-human patterns and automatically alerts the administrator when it detects any bot activity or potential fraud activity.
- **Expert users** — Cybercriminals practice a proficiency with keyboard shortcuts and function keys which are not typically seen with real users. The variable expert user will help us to identify users with expert proficiency in filling the application form hinting that the user had filled this form before many times and raises the flag for potential fraud.
- **Low data familiarity** — A genuine person filling out the application form to open the account for the very first time is most likely to enter his/her details rather than just copying it from somewhere and those entering stolen personal information are more likely to cut and paste data that would be intuitive to the legitimate user. This variable allows us to judge the familiarity of users with the data entered in the application form.
- **Machine/bot activity** — this variable can be used to spot criminal behaviours in the application flow, even if the access is from a new device/IP, and it can reduce manual reviews without deterring legitimate new customers.
- **Time to Complete** — the time taken by the user to complete the application form from start to finish will be an important factor to determine whether a particular individual is more likely to commit fraud or not. If the time to completion is very less than it shows that user has higher familiarity with the application procedure and he/she might be a potential imposter.

Credit Bureaus and Credit Application Data

A credit bureau is a company that collects and maintains individual credit information and sells it to lenders, creditors, and consumers in the form of a credit report. User credit information along with credit card application data can be used for identifying new accounts fraud applications:

- **Mode of application** — if particular account holder previously applied via offline form and new application is online (or vice versa) then it might be a fraud credit card application.
- **Spending Behaviour** — the spending behaviour of previous credit cards can be compared with new credit card, its behaviour is not similar then there is a high probability of fraud.
- **Location of spending** — People spend (mostly) where they live, work or travel, if the locations of spending on new credit card if different than previous transactions than there is potential of fraud.
- **Location of application** — if application is offline than location (branch) where application was submitted can be an important variable to determine the fraud. Eg- If I work in Gurugram and my hometown is Pilani but if a credit card application from my account is submitted in Pune than there is chance of fraud.
- **Credit History** — if a user has no credit history, someone like framer or self-employed labourer, he probably won't apply for credit card.

Bank Accounts Details

Accessing one's bank account details and finding patterns such as online spending patterns, monthly expenses like fuel, groceries, etc. can help to find randomness in user behaviour.

- Credit card usage history : If an individual has an existing bank account in the same corporation as the credit card issuer, the spending habits can be analysed to detect anomalies in purchases on the new card
- Account creation date: The older the account is, the less will be the risk of having any fraud attached to the account.
- Transaction Geolocation history: If the credit card purchase geolocation history does not match the geolocations from other purchases, for example, the details obtained from the United Payments Interface (UPI), a potential fraud might be occurring.
- Average bank balance: We can access the information about the average bank balance of the account.
- Online Spending pattern: This helps in gauging user behaviour towards online spending and can filter out any random transaction easily which can be a fraudulent one

Online Credit Fraud

With the rise in the telecom industry a very high percentage of people now having access to the internet, mobile data usage. We need to be a bit more careful when saving our online data and sharing it. Our mobile phones are filled with personal details and even account information (exactly what online fraudsters are looking for). They can easily hack into our data with sophisticated tools to phish.

- **Avoid transacting on a public Wi-Fi**: Refrain from making any payments or transfers online when accessing public Wi-Fi. A hacker (connected to the same router) can tamper with your transactions. If you are looking to make an important time-sensitive transaction, simply opt for a cellular network.

- **Minimize the exposure to your personal details online:** Think twice before uploading any personal document on any social media or online forums. Details such as your PAN, Aadhaar card, account number, and card numbers can be used by scammers to even open a loan account in your name. And you wouldn't even know until you start getting calls from collection agents

- **Use encryption and tokenization to mask your details:** This is perhaps the simplest and most effective form of stealth, wherein your card is taken by the salesperson for swiping and the information from the magnetic strip is copied to be used later for illegal transactions. Recently RBI directed card network companies such as MasterCard and Visa to offer tokenization services. Tokenization helps encrypt your 16-digit card number so that this is not revealed to merchants and strictly remains with your card issuer.

- **Monitor your credit score regularly:** Though there are multiple sections in the report, your 'accounts information' section holds the details of all the credit that you have availed till date. Check this section for accuracy and if there is an account that you do not recognize as your own, it could be a case of identity theft.

- **Pharming**: In this technique, fraudsters reroute you to a fake website that seems similar to the original. So, even as you conduct transactions and make payment via credit or debit card, the card details can be stolen.