USSD – An underutilised data resource in the fight against syndicates

USSD stands for Unstructured Supplementary Service Data.

Wikipedia defines USSD as follows:

"*A protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for WAP browsing, prepaid callback service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network.*"

Think of any value ad services where your customer can communicate with your systems, for example when they send an SMS to your systems to enquire about the status of an application or available balance and so on. USSD data is the data generated during these interactions between your client's cellular phone and your systems. This data will include text data containing the requested information as sent by the client (including the identity number of the person and/or account number to which the query relates) and the text data sent back by your systems. But the most crucial information contained in this data is the cellular number from where the request came.

Before we continue, here is a tip when doing data mining in order to detect syndicate activity:

Ask yourself what makes your client a unique entity in your data or on your company's systems? Is it their identity numbers? NO! Is it their full names? NO! Is it their bank account details? YES! Is it their contact details? YES again! A syndicate will already have complete customer profiles printed from your systems. These they either obtained via key-logger, inside person or interception of data/documentation…the possibilities are endless. BUT, what is key here is the bank account detail and contact details. They want their hands on the money and if you decide to phone for security purposes (you now those pesky security questions) they want you to phone them and not the actual customer. Now read further to get things in perspective.

Note: *If you are in the business of delivering goods or services to customer addresses, then the delivery address of your client will also form part of those details which make your client unique on your system.*

If a syndicate phished/cloned your customers' accounts you must ask yourself where and how can the syndicate establish whether those accounts are still active? The customer might have realised that he was a victim of cloning/phishing even before the syndicate was able to use the cloned cards. Thus, the syndicate is running the risk of having egg on their face when trying to use the cloned cards. Some organisations have facilities where you can make an enquiry via a SMS to establish available credit limits and this is where USSD information is crucial for you to detect potentially cloned/phished accounts.

Perform these initial data mining procedures in order to search for syndicate activity in your data:

1. Obtain the USSD data and perform a count of how many times each incoming telephone number can be linked to more than one unique account (easily done in Excel with pivot tables and a few easy if-statements). If you get hits of 2 or more, you are onto something. This is very much the same way you identify potential fraudulent payments to fictitious suppliers, i.e. by summarising all payment transactions according to the bank account numbers and then listing those bank account numbers which can be linked to more than one unique supplier. I can guide you through the Excel formulas required to do this – it is basically one *if*-statement and a *pivot table*.

2. Obtain incoming call logs of your call centre and the call centre's logs regarding call centre staff user activity on the systems. By performing a link between the incoming telephone numbers and the account to which the call centre staff gained access during that call you will be able to determine whether an individual phoned in to enquire or make changes to more than one account.
3. You can build "red flag" reporting into your call centre systems. Include the USSD and incoming call history for a significant period. These reports can then generate on a daily basis:

   - A report indicating all accounts being accessed from a single telephone number via USSD related functions and actual calls to the call centres;
   - A report indicating the changes made and by which call centre staff[1] these changes were made (there may be a trend indicating that a specific call centre employee is assisting the syndicate); and
   - A report indicating potential customer accounts which could soon be targeted by the syndicates.

4. The abovementioned reports should be reviewed on a daily basis. Verify any changes made to bank account details, contact details and delivery addresses shortly before the potential syndicate related activity was noted. I recommend that you try and contact the customer on the contact numbers preceding the "updated" contact details (i.e. phone them on the old numbers first). If they answer on the old number you can confirm with them whether they recently contacted your company to make changes to their profiles etc. There are also various websites available where you can test email addresses, i.e. the website "pings" the email address provided and will provide you with feedback on whether the relevant email address exists. A lot of customers could have the emailing function activated on their cellular phones and could be receiving updates from your system when changes or purchases are made on their profile…the syndicate won't like this and would thus provide a bogus or alternative email address.

The lesson here: There is more data available on your systems than the little bit you have access to via your BI systems (BI refers to business information or those sets of data utilised to generate operational business reports). Gain an in-depth understanding of your processes and the data generated at each stage where you, your customers, your staff and the systems interface with each other. Refer to www.crisp-dm.org for a nice schematic setting out a proper data mining process.

I hope this helps. Otherwise phone or email me and I can guide you through some practical examples. I recently conducted awareness sessions on the above (in more detail) and 2 weeks later some attendees phoned me to confirm that they actually had positive results on this topic. Give it a try!

[1] Some things I have learned from past experience with call centre staff are this: They can be very naïve when dealing with callers (usually due to a lack of proper training and awareness); they are not very loyal to a brand or the company they work for as they are often viewed as temporary staff and staff turnover is high within call centres; they are paid minimum wages (if they are lucky); their loyalty is also negatively impacted because their every movement are closely monitored and policed by their managers (sometimes they are even required to clock in and out for toilet/smoke breaks); but they can be effective in your fight against fraud and syndicates by ensuring proper training, awareness and guidance.

Furthermore, a recent client of mine in the micro-lending industry were targeted by a card cloning syndicate. The fraud suffered by them peaked at R12 million for the month. I assisted them in performing a fraud review or "fraudit" (my term for an in-depth fraud audit/review of a process which took 1 week). Within 2 months after implementing some "red flag" reporting based on the stuff discussed above, the fraud reduced to R2 million in the 3rd month after my involvement. My fee for my involvement was approximately R60 000…now that was a nice investment!