Learning Lab LAB1 T-11: Identity War Games

Post-Conference Summary
# Table of Contents

**BACKGROUND** ................................................................................................................................................................................................. 3  
  Objectives ................................................................................................................................................................................................. 3  
  Set-Up and Rules of Engagement .............................................................................................................................................. 3  

**WHAT WENT DOWN IN THE LEARNING LAB** ................................................................................................................................. 4  
  The Identity War Games Scenarios .................................................................................................................................................. 4  
  Discussion Points .................................................................................................................................................................................. 4  

**TAKEAWAYS** .................................................................................................................................................................................... 5  
  Overall highlights ............................................................................................................................................................................... 5  
  Some specific considerations .......................................................................................................................................................... 5  

**CONTACT DETAILS** .......................................................................................................................................................................... 5
Learning Lab Summary

Background

Objectives
The Identity War Games learning lab was designed to provide a highly interactive way to learn about online account opening fraud, one of the emerging threats to digital transformation, and the various data sources organizations can now use to fight it.

Banks, credit card companies, government services and any digital service requiring an identity check - struggle to fight Account Opening (AO) Fraud, which has seen a dramatic increase in recent years. Know Your Customer data verification is no longer working as criminals have hacked into every major identity related database, or alternatively deploy synthetic ID schemes.

This learning lab provided the audience with a collaborative experience in which best practices are exercised, new data sources are demonstrated, and the process of fast identity decisioning is practiced.

Set-Up and Rules of Engagement

- The audience was divided into 8 tables with 5-7 team members per table.
- Each table acted as a fraud team. The team’s objective was to reach the quickest correct decision about identity questions during several real-world new account scenarios.
- The moderators first presented some basic facts about the scenario, and then began presenting additional Data Points, one by one.
- After introducing each new data point, internal discussion was allowed at each table; every team member had an opportunity to share their insights and analysis with the team.
- When the moderator asked for the team’s decision, each member casted a personal vote, selecting from one of three options:
  - This case is definitely FRAUD!
  - This case is clearly GENUINE!
  - Inconclusive... We need more DATA!
- A table had to have at least 3 people supporting a FRAUD or GENUINE decision to make that call.
- Once a table (representing a fraud team) has made a final call – i.e. saying they believe the case to be definitely Fraud or definitely Genuine – they are not given further data points and only at the end of the scenario they know whether they’ve made the right call.
- This set-up created a healthy competition between the tables, with each ‘fraud team’ trying to be the first to have a correct call on the scenario.
What went down in the Learning Lab

The Identity War Games Scenarios

Following some general explanations about online account opening (AO) fraud, the data sources the industry now uses to fight it, and some practice scenarios, we presented three scenarios:

- **Call the Dead Guy**: In this devious scenario, based on a real-world case, the fraud teams got early indication that the SSN provided by the applicant belongs to someone who died 10 years ago. However, further data focusing on behavioral biometrics showed that the user was highly familiar with the data they enter and generally behaved like a very genuine person. Fraud teams who made an early ‘Fraud’ call discovered that relying just on KYC checks may actually lead to false rejections of users, as in this case the user had a typo in the SSN – leading to all the red flags.

- **Defying the laws of physics**: A ride sharing app user account is at risk: someone used their credit card to open a new account and order expensive rides in Singapore, Hong Kong and Thailand, at the same time that the user was using the app in San Francisco and Los Angeles area! The fraud teams discovered that social media can provide valuable clues as to the identity of the culprit, who in this case was the user’s girlfriend. Several fraud teams had an early hunch that would be the case and made an early call of ‘genuine’ – which was correct.

- **Saving the Sea Turtles**: A strange order is made at an eco-friendly paper straw online retailer. Almost 1 million straws are to be shipped urgently to the middle of the pacific ocean! Is this a genuine order or a peculiar fraud case? In this scenario each data point was more incriminating than the previous one – starting from the weird initial facts, through bogus delivery addresses, and ending with behavioral biometric analysis showing complete lack of familiarity with the personal data of whoever made the order. This was an actual fraud case, albeit quite mysterious as paper straws are not sellable items; we also explained the criminal’s MO – which was actually not focused at all on the straws, but rather the inflated $10,000 shipping bill.

Discussion Points

In between working on fraud scenarios, several discussion points were raised by either the moderators or the audience, generating a healthy debate. Here are some of the highlights:

- **What’s the cost of a false decline?** The attendees all agreed that high friction risk controls and relying on data and tools that generate a high degree of false positives can generate significant lost business. Digital Onboarding should be a smooth experience and applicants may not try again, and end up applying with a competitor. In addition to the direct loss of business which limits the portfolio’s growth, there are also heavy operational costs. Digital acquisition requires limiting false declines to a minimum, and this can be done by taking into account multiple, independent data sources and controls.

- **Is social media helpful?** The verdict was mixed. Most attendees said investigating social media is a highly manual process, but it might salvage some false positives or lead to a stronger view on fraud cases.

- **How can a site collect behavioral biometrics data?** A questions from the audience was about collection of behavioral biometrics, often cited as one of the most effective next-gen data source for fighting account opening fraud. Banks, credit card companies and other organizations use a Java Script to collect keyboard and mouse behavior, touch and accelerometer data. iOS/Android
apps have an SDK library that collects similar data points. This can be used in a rule-based system, or Machine Learning-based models that look at things like: is the applicant familiar with their own personal data (they should be)? Is the applicant familiar with the onboarding process (they shouldn’t be as they do it for the first time)?

Takeaways

Overall highlights

- There are a variety of data sources to review:
  - Resource Correlation (Email, Phone)
  - Device and Location Reputation
  - Social Media and Digital Footprint
  - Behavioral Biometrics
- Decisions are increasingly complex – but more insightful
- It’s never a single incriminating fact – multiple data points need to be considered

Some specific considerations

- KYC controls look for many correlations and try matching many factors, but sometimes the data is biased, faulty, not up to date – or the user just makes a mistake
- Using next-gen data sources that don’t actually use the data itself can provide a ‘second opinion’ that clears applications, leading to higher acquisition rates
- Having multiple layers of visibility is key
- Social media analysis can provide negative and positive clues, but may be difficult to fully automate and easy to get into a rabbit hole if you’re not careful
- The bigger the transaction, the higher the risk, but also the higher the reward. It’s very difficult to make a good call without sufficient data
- Which is why just transactional data is considered insufficient. It takes many layers of analysis to make an informed decision

Contact Details

LinkedIn: Uri Rivner
LinkedIn: Erin Englund