How to Get Insights About Individual Customers Before the Know-Your-Customer (KYC) Phase?

Pre-KYC Identity Matching for Digital Banks and Other Digital Service Providers to Boost Acquisition

Reading Time: 7 Mins

lynxanalytics

Introduction

Most people would say that the trackable lifecycle for a digital customer starts after some form of KYC process has been completed. That is once a reliable customer ID (e.g. social security number) that is unique and immutable, can be attributed.

However, a lot of potential customers never make it through the KYC process; customers for whom you do not necessarily capture data but that could prove very helpful in understanding and optimizing the acquisition process.

That is why it is extremely valuable to identify unique customers before completing the KYC process. You obviously would like to know, if you have a fixed acquisition budget, who should you target to acquire the largest customer value portfolio (combination of take-up rate, future spending, future churn, future costs). If you want to use predictive analysis and machine learning, you must do an extensive pre-KYC identity matching.

By the end of this guide,

you will learn how to…

- Gather useful customer profile information before the KYC process
- Use that preliminary information to improve customer acquisition
- Understand the pros and cons of different customer ID types
- Determine the ideal unique ID for your customers

MSISDN / Email Address

One of the best personal identifiers is the phone number, also known as the MSISDN. You will certainly acquire a phone number after the KYC process, but it is possible to obtain it before that.

For example, phone numbers will be available during the lead generation phase if you are running SMS campaigns with bulk numbers. It is also possible that some potential customers are using SMS or voice channels to enquire for information or sign up. Your inbound/outbound call centre can be one of the best sources of highly-qualified leads along with MSISDNs. Usually, there is a lot of information already embedded into the digits of the phone number (mobile or fixed line, brand, type, location, etc.)

Of course, a given MSISDN and a post-KYC-ID do not necessarily form a one-to-one relationship. A customer can register with one phone number, and then decide to provide another number during KYC. Thus, it is very important to follow and analyse MSISDN – ID relationships, using graph analytics for example.

An email address is very similar to a MSISDN. You can obtain email addresses pre-KYC, during the marketing process, app download, web-download or during registration.

Device ID

Every phone has a unique identifier, known as the IMEI (International Mobile Equipment Identity). This unique code can be accessed every time a customer has a digital interaction (e.g. downloads an app, opens an app, uses an app, etc.)

The IMEI is available even if the customer is not using a SIM card during the interaction. Of course, the IMEI will change every time the device is changed or if multiple devices are used.

Thus, post-KYC, the device – ID matching can be a many-to-one relationship. Unfortunately, for some unbranded mobile phones the IMEI is not unique; in some cases hundreds or thousands of devices can inherit the same IMEI. On the other hand, the IMEI hierarchy is very logical, and you can derive a lot of information using IMEI dictionaries (phone brand, type, release year, etc.)

IDFA and Cookies

Some technical protocols have been created to follow digital ads and click-throughs. For mobile devices, Google and Apple have introduced the Identifier for Advertisers (IDFA), which is a unique ID for every device / account. It was introduced to maintain a vibrant advertising ecosystem without the need for personal identifiable information. The IDFA can be muted or re-generated, so if your customer turned it off on his/her phone, changed it, changed profile, or switched phone, you will not be able to trace this customer back in time.

Nevertheless, this is probably the best way to track customers from ad impressions (when the first display advertising was shown), to click-through, to download, to registration, and finally KYC. The IDFA is accessible at every digital interaction.

Because of its uniqueness, it is very likely to have a one-to-one relationship with the post-KYC ID, or maybe a two-to-one relationship if the customer has two devices with the app installed and is using both devices. IDFAs can be used as inputs for ad platforms to generate look-alike audiences similar to your existing customers in order to achieve higher conversion rates.

Laptops and desktops do not support IDFA, but cookies can be used in this context as they perform a similar role.

Name and Address

A name and address usually don't have a properly structured form and are not necessarily unique, so those typically don't perform well as customer IDs. But it does not mean we cannot use them during the identity matching process. In many cases, these fields can validate or falsify identity matches.

Names often overlap with the email address and home and work addresses can be validated using geo-location tags obtained from the app during digital interactions with the customer.

Rewards Program Membership ID

It is possible that a new customer is referred to you via a rewards program partner or an affiliate program. In this case, the program membership ID as well as some preliminary profile information collected by your partner can be used to uniquely identify a customer before the KYC process has been completed.

In some cases, the profile can be rich enough to validate other pieces of information you might have collected such as MSISDN, email address, etc.

The Ideal Post-KYC ID

Finally, let's look at what would work best as a post-KYC ID. Of course, every company can assign a new ID to a customer and try to keep it as unique as possible.

It can be connected to multiple other IDs, assuming they can be matched easily. In any case, a unique, immutable, general, and unchangeable ID (or a hash from that ID) should be used.

Fortunately, many countries now have their own system for unique citizen IDs (e.g Indonesia has NIK, Singapore has IC/FIN, Hong Kong has HKID), which can be used to establish unique customer IDs.

Conclusion

The various IDs presented above, coupled with machine learning techniques, can provide insights on the nature and value of a potential customer before the KYC process has been completed. In turn, this information can be used to optimize the marketing budget for acquisition and improve the qualification and conversion rates.

lynxanalytics

Are you a digital bank or digital service provider looking to boost adoption for your products?

Get in touch with us today to explore how we can help you with our data science solutions.

Yes, I'm interested to learn more