Digital Customer Onboarding
Easy to Use Checklist

for Individual Customers (natural persons)

1. Front-End (what your customer sees and needs to provide)

1.1. Ask the customer to fill in the following fields:

a. Full name
   - ⇒ Offer two separate fields (First Name, Last Name), because otherwise for some countries you won't know which one is which.

b. National or foreign ID type and number
   - ⇒ To collect ID type, it is better to offer a drop-down list with the following document types: passport, national ID, driver's license. Many clients ask me if they should offer "other" category for rare document types such as diplomatic or marine passports, asylum certificates and other possible document types. For a young startup with limited resources I would advise against it, because if you offer "other" category, you need to continuously research it and spend time reviewing it, which is not necessarily what you would like to do.

c. Residential address
   - ⇒ It is better to offer a drop-down list for all countries from where you are ready to accept the customers and not even display the countries that you don't support.

d. Date of birth
   - ⇒ If you offer financial services or other regulated products, it is better to include field validation logic and ensure that your customer is 18 years old.

e. Place of birth (country)
   - ⇒ Offer the drop-down list and include all countries (recognized by the UN or by the country where your platform is setup.

f. Nationality
   - ⇒ Offer the drop-down list and include all countries (recognized by the UN or by the country where your platform is setup.

g. Phone number
   - ⇒ Offer country prefix drop-down list and decide if you would like the phone prefix to be only from the country of your customer's residence or from any other country.
   - ⇒ You can decide if you would like to confirm it (strongly recommended) by an SMS code.

h. E-mail (confirm by reverse link)

1.2. Uploads:

- ⇒ **Proof of Identity:** Valid ID document (passport, driving license, national ID card, where applicable – front and back pages).
- ⇒ **Proof of Address that is 3 months old or less:** utility bills, bank statement, phone bills, credit card statements, insurance statements, childcare invoices or any other document that has a recurring nature and indicates an ongoing relationship between the customer and the sender

(e.g. school certificates, letters from the university), official letter addressed to this address or correspondence from government agency, confirmation of property purchase. Sending verification code to the customer address can be an option.

1.3. Accept T&Cs and Privacy policy

⇒ When your customer has completed their registration, they have to accept your T&Cs and Privacy Policy.

⇒ You need to implement 2 separate tick boxes (or click buttons, or similar): for T&Cs and for Privacy Policy; and you cannot pre-tix them. The customer must actively accept each of them.

⇒ This is the moment when the customer becomes a customer and we can store their info, send them a welcome email, confirm their registration, send them reminders, place cookies for security (or marketing) purposes, if your Privacy Policy discloses this fact. From this moment on, you have an obligation to protect their account security and integrity.

1.4. Sending an email confirmation

Send a message to the customer confirming that their account has been registered. Ask for email confirmation (if not done so before). Now you can add instructions on how to activate the account, how to add a payment instrument, navigate the website, how to contact the support team, etc.

2. Back-End (what you do and how you check the details provided by the customer)

2.1. Onboarding checks

During the process of client onboarding (e.g. client registration) the following information will be provided by the client and the following checks should occur automatically (close to real time) to ensure you are performing sanctions and PEP scanning obligations and also for the purposes of managing online fraud risks:

Customer Data	"Silent checks" – not visible to the customer	Follow up
Full name	- The full name must be scanned against all applicable to you sanctions lists for SDN, sanctions and PEPs (you can use services, for example, by Veriff, ComplyAdvantage, WorldCheck, Trulioo, Passfort, Jumio, Onfido[1]) - Optional (for example, you could only use it for PEP or high-risk customers) – full name can be scanned against negative media references (corruption scandals, bankruptcies, litigations, change in control, M&A announcements) – e.g. by RDC, Passfort, Onfido, ComplyAdvantage (be mindful, this functionality could generate a lot of false positives and should be used wisely) - Full Name is scanned for obviously false names, e.g. Coca-Cola, Peter Pen, celebrity names, obviously abusive and oblivious names (e.g. batch scanning).	- If there is a partial match from scanning, an account must not be able to transact, until the issue is researched and resolved.
Date of birth	- Validation that the client is 18 years old	- Block if the client is under 18
Address	- Ensure that the address is from an eligible country - Check consistency between IP, geolocation, residence address and possibly phone prefix. - Detect if VPN or other disguising techniques were used	- Flag inconsistencies and decide what you would like to block or escalate for manual review
Nationality	- Flag cases where nationality is different from residence country	- Decide if you would like to ask for the proof of visa/legal status in the country
E-mail	- Confirm email address by reverse link - Detect temporary emails and bots - Scan if email is listed in the known lists of compromised credentials	- Flag bots and temporary emails.

[1] https://onfido.com/
www.trulioo.com
www.passfort.com
www.complyadvantage.com
https://veriff.me/
https://www.jumio.com/

	- Scan emails for references in commercial registers, social media and other public databases	
Phone number	- Check consistency with country info, flag inconsistencies	- Avoid using SMS for 2FA, better to use authentication app, since it requires separate authentication when installed.

2.2. Ongoing Checks

Here are additional examples of information that could be collected and continuously analyzed at the point of registration and going forward by using various transaction monitoring tools[2] in order to detect suspicious activities and manage the risks of online fraud:

⇒ Are there signs of malware, viruses, etc. on the device used for registration and have you seen this device or this IP before and whether or not it was associated with a problematic situation.

⇒ "Machine fingerprint" – e.g. device ID, operational system, language settings. The device used for registration is usually a very good data point for future detection of account takeover and fraud prevention.

⇒ Detect instances of same device used, same IP used, same address used and any other data points matches in order to flag linked accounts.

⇒ Velocity monitoring: you should have rules and specific logic to be able to generate certain system alerts based on changes in the customer behavior, such as sudden increase in volumes, recently added or never used funding instrument used for withdrawals, payments to higher risk destinations and similar.

⇒ For physical shipping of goods, it is important to detect and analyze mismatches between the shipping address and the billing address, detect unrealistic addresses, postal codes which are associated with high levels of violent crimes, or whether there was a previous successful delivery or undisputed transaction to that customer address.

⇒ Behavioral biometric. How customers type or move their mouse can be an indicator of identity theft and account takeover.

⇒ Custom lists: It is possible and often useful to create and maintain special lists, such as "abuse list", "high risk list", "VIP lists" to appropriately react to certain customer activities, detect and prevent repetitive fraud, etc.

[2] www.kount.com
https://pipl.com/
https://simility.com/
https://www.clarus.io/

2.3. Blockchain Tracking

It is possible to risk-score the blockchain history of the bitcoin address used by the customer by using Elliptic AML tool[3] or Chainalysis[4]. These tools are able to analyze the overall blockchain history of the address used by the customer for making a transfer. The following factors are among those analyzed to produce a risk-score for each case at a given point in time:

⇒ Was this address involved in disguising techniques, such as using "mixers" or aggregated accounts.

⇒ Was this address ever connected with a known "bad" address and if so, what was the total % of volume of those transactions.

⇒ Is this address connected to a known mining pool.

⇒ Is this address receiving funds from a known custodian or reputable crypto exchange and of so – what is the % volume.

[3] https://www.elliptic.co/

[4] https://www.chainalysis.com/