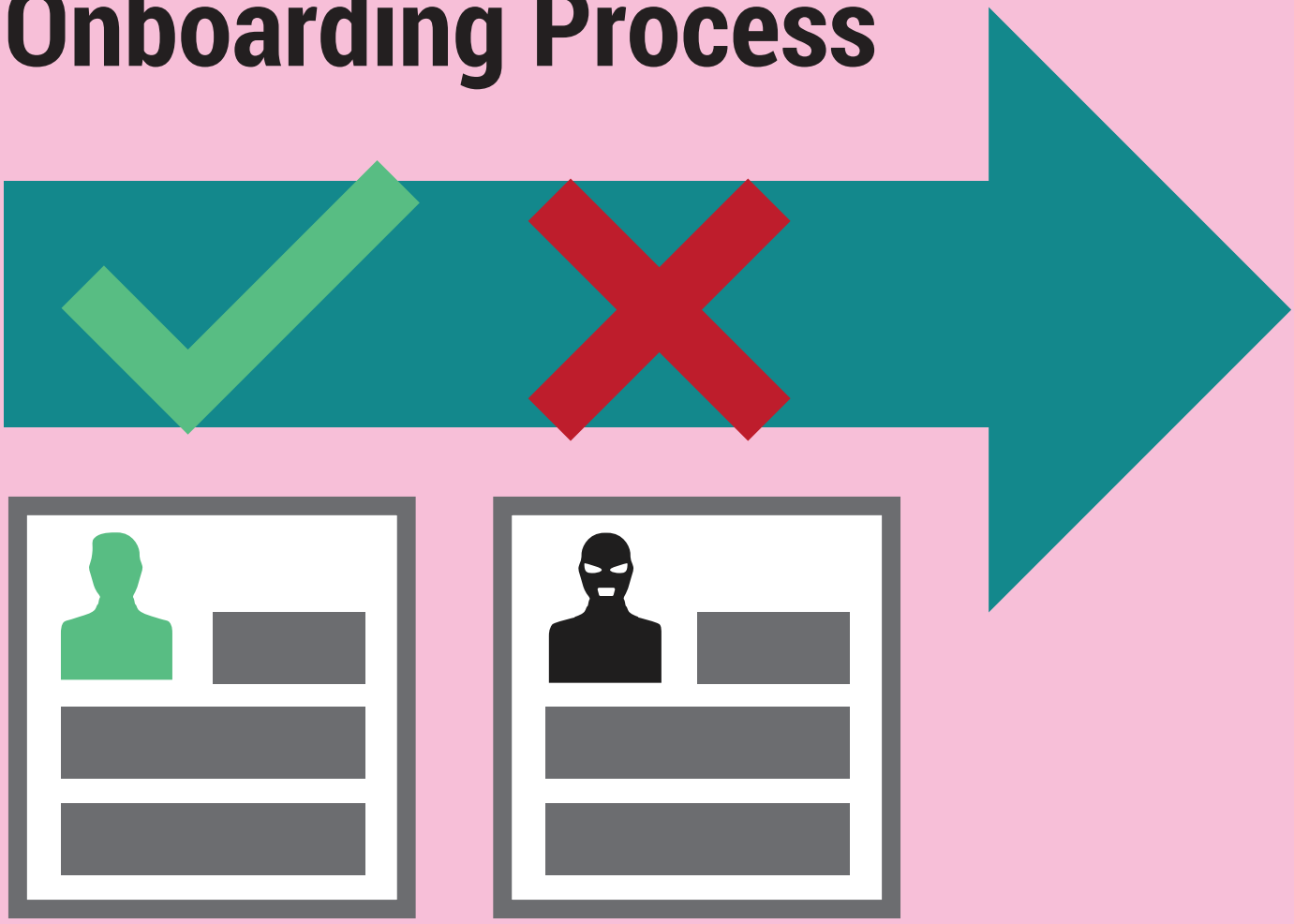
IdentityMind GLOBAL

WHITE PAPER

# 10 Best Practices for Fraud Mitigation in the Lending Onboarding Process



# BEST PRACTICES FOR FRAUD MITIGATION IN THE LENDING ONBOARDING PROCESS

When The *Wall Street Journal* reported last year on the remarkable increase in commercial lending rates, it also postulated that business loans originated through alternative lenders, just P2P (peer-to-peer) is expected to reach ~**$37B by 2017** (Morgan Stanley – "Global Marketplace Lending" 2015).

Whether or not that prediction comes true, the outlook for the online lending industry is bullish. However, times are also bullish for cyber criminals using stolen identities to appear legitimate during the underwriting process.

When applicants only appear online, fraudsters can use stolen information to compromise lenders' ability to verify applicants' identities. Traditional fail-safe measures such as conducting background, identity and credit checks can fail because the lender is checking an application against legitimate identities. This increases the risk to the lender's bottom line and to its ability to comply with Know Your Customer (KYC) provisions of the USA PATRIOT Act's requirement for an effective Customer Identification Program (CIP).

An onboarding process that follows industry best practices for CIP must include risk-based procedures for verifying the identity of each customer, whether consumer or business. At a minimum, the lender must obtain the following from each consumer before opening an account:

- Name
- Date of Birth
- Address
- Identification Number
  (e.g., a taxpayer identification number for U.S. citizens, a passport number for non-citizens)

For a "person" other than an individual (such as a corporation, partnership, or trust), the lender should obtain documents showing the legal existence of the entity such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

The lender must also supplement the process with risk-based verification procedures "to ensure that the bank has a reasonable belief that it knows each customer's identity." (Source: U.S. Dept. of Treasury)

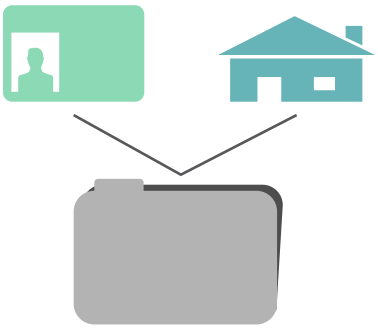
Filtering out fraudulent applications during the underwriting process requires taking steps such as analyzing the names, roles and relationships on the application, considering the behavior of the applicant and known history, and determining whether the applicant is linked to fraudulent activity.

# The 10 best practices every lender should follow

to mitigate fraud in the underwriting process:

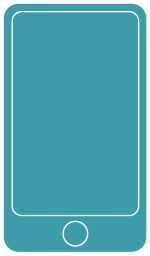
## Identify Verification

There are several ways to verify an applicant's identity.



### 1. Match application information to trusted sources of information:

- Is the applicant's Social Security Number valid?
- Does the applicant's date of birth information match the DOB associated with public data? Can it be connected to the applicant's name via public records?
- Is the home address risky?
  (i.e., prisons, warehouses, hospitals, universities)
- Check to ensure the address has not been associated with fraud.



### 2. Check phone records:

- Is the presented phone number valid? Get the phone's carrier, city and country where the applicant's phone is registered, does it match the number associated with the user's public data?
- Examine the actual type of phone the applicant uses to make sure it's not considered unsafe.
- Run a simple test by sending a PIN to the phone number on the application.

### 3. Verify email addresses:

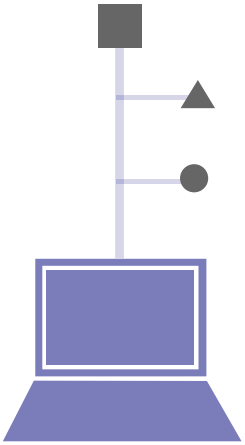
- Have you seen the applicant's email address before?
- If so, when was the first time your system recorded it?
- If the email address has not recorded much activity on the Internet, that should raise a red flag.

### 4. Verify billing information:

- Does the billing name and billing address match private databases or public records?
- Confirm the information does not appear associated with someone public records indicate is deceased.
- Confirm the billing country is on your acceptable country list.

## Check for Signs of Identity Theft or Serial Fraudsters

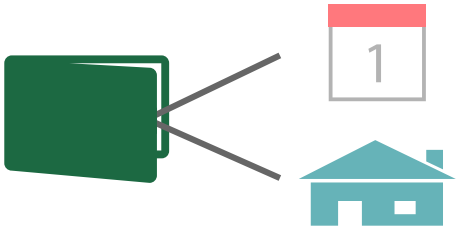
Even the most careful criminals cannot cover all of their tracks.



### 5. Examine device history:

- Determine the date when your system saw each applicant's device for the first time.
- Identify the number of devices associated with the application's user account.
- Verify that none of those devices failed previous validation checks.
- Confirm the number of applications associated with each device, as well as the number of user accounts.

### 6. Confirm funding payment instrument:




- Ask the same questions you do when examining an applicant's devices.
- Research the date when your onboarding system saw the applicant's funding payment instrument for the first time.
- How many user accounts are tied to it?
- Verify the billing address, and find out the payment reputation.

### 7. Check your black list:

- Are any application parameters on your watch or black list?

## Analyze Geolocation

Triangulate based off IP address, phone number, card issuing, and billing information

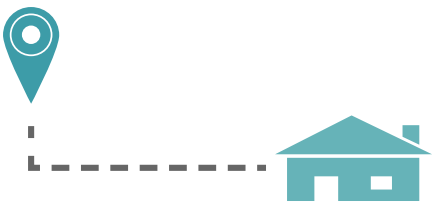
### 8. Review the IP address:

- Get the city, country and ISP associated with the applicant's IP address.
- Check whether the state and country is on your list of acceptable for regulation purposes
- Figure out what type of device it is (e.g., desktop PC, smartphone, tablet, laptop, gaming console, and even a smartwatch).

**123.45.78.9**

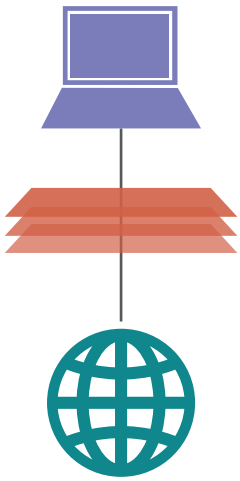
### 9. Do the math:

- Calculate the distance in miles between the IP and billing, account and shipping addresses.



**10. Confirm the Proxy:**

- Is it coming from a known non-corporate proxy, or is it using an anonymous proxy?
- Is the IP address a bad proxy or have a high risk score?
- Is the device using a Tor browser on the Tor network?
- Is the applicant's traffic from a bot?
- A "yes" answer to any one of these questions should raise an immediate red flag.



## Conclusion

The speed and overall volumes of loans made through alternative financing make the industry a prime target for fraud. The goal must be to catch fraudsters before they cheat lenders, and at the same time it is important to minimize unnecessary delays and authentication methods that introduce customer friction. It is also critical to avoid false positives reflecting incorrect identification, which deny financing to good customers. By staying up to date with onboarding best practices that include strong identity verification, checking for telltale signs identity theft and serial fraud, and incorporating updated strategies for establishing trusted digital identities, lenders can expedite the loan process for good customers, while stopping bad actors early in the process.

**IdentityMind Global's ONBOARD initiative can reduce fraud losses and streamline your onboarding process. Contact us to learn more.**

**ONBOARD**
**ACCOUNT ONBOARDING PROTECTION & COMPLIANCE**

To schedule your demo, reach out to us at **sales@identitymind.com**.

If you have questions or comments about this white paper, or would like to see other use cases, feel free to contact us through twitter at **@identitymind** or send us an email at **evangelist@identitymind.com**.