Detecting fraud in new account applications

Fraud detection that works better for your customers—and your business

Is your fraud detection system helping or harming customers who want new accounts? And how can you harden your system against today’s savvy fraudsters?

To answer these questions and more, start by identifying gaps and uncovering opportunities in your current system.

Use the checklist below to get started; add questions of your own to pinpoint the unique needs of your financial institution.

1. **Identity verification**
   Identity verification confirms that an applicant’s details match historical records. As identity fraud becomes more sophisticated, intuitions are augmenting identity verification to reduce manual reviews.

   Who is your current identity verification provider?

   **Provider:** ____________________________
   or □ I'm not sure.

   What percentage of applicants requires any type of manual review based in the results of current identity verification methods?

   Based on the number of manual reviews required and their associated costs, how would you rate your satisfaction with the identity verification methods used in your fraud detection system?

   ![Identity verification checklist](in_table)

   **My rating:** __________________________

   If you selected a rating of 1 or 2, what factors contribute to your dissatisfaction?

   __________________________

   In addition to identity verification, does your system use tools or methods to analyze patterns of identity behavior to detect suspicious usage of an identity?

   □ Yes □ No
If yes:
- Box Results are delivered and associated with identity verification responses
- Box Results are delivered separately and must be manually linked to identity verification responses

2 Device verification
With ID theft more prevalent today, analyzing both an account applicant and the device being used can more quickly identify hard-to-detect—and costly—fraud attempts.

Are you using device verification to profile the risk of the devices that applicants use to open accounts in faceless channels?
- Box Yes
- Box No

Who is your current provider, if any?

If you are using device verification, does it examine the following? (Check all that apply):
- Box Advanced geolocation
- Box Known reputation
- Box Advanced device profiling
- Box None of the above
- Box Other ____________________________

Do your device verification methods assess devices and consumers together for risk, or are the pieces looked at in isolation?
- Box Together
- Box Isolated

If they are looked at in isolation, does this require you or your team to engage in manual reviews?
- Box Yes
- Box No

3 Identity authentication
Authentication ensures that applicants are who they claim to be—typically by asking questions drawn from personal information. Smart authentication relies on multiple data sources and matches the transaction’s risk level.

Are you using multi-factor authentication for additional confirmation in faceless channels?
- Box Yes
- Box No

Who is your current provider, if any?

Do you use the same authentication process for all consumers, or do you tailor authentication based on consumer or transaction risk?
- Box Same
- Box Tailor

Are multiple modes of authentication available?
Or must all consumers pass a knowledge-based exam?
- Box Multimode available
- Box Must pass knowledge-based exam

Share your results with your team to identify opportunities to boost your fraud detection systems and to incorporate new solutions.

LEARN MORE
Looking for assistance to review your current system? Contact us today at 844-245-4071. We’ll work with you to map your current state and identify gaps and opportunities.
Solve today’s most common (and problematic) approaches to fraud detection

At TransUnion, we’ve helped hundreds of financial institutions stop sophisticated fraud and improve the customer experience. Here are some common approaches we hear financial institutions say present the most challenges, the potential impact of these approaches and the TransUnion solutions that can help.

<table>
<thead>
<tr>
<th>COMMON APPROACH</th>
<th>POTENTIAL BUSINESS IMPACT</th>
<th>TRANSUNION SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relying primarily on verification to detect fraud.</td>
<td>With the frequency of data breaches rising, savvy fraudsters have constant access to new and inexpensive stolen identities. But until those identities make it into databases of known fraud, traditional verification will not recognize a threat.</td>
<td>TransUnion Identity Alerts, an easy and cost-effective add-on to a credit report, can bolster traditional verification. Using sophisticated analytics and real-time, cross-industry data, this solution looks for patterns of suspect activity to flag identities that are likely being misused or show unusual association to other identities—even if they don’t appear on lists of known fraud.</td>
</tr>
<tr>
<td>Reacting to new regulations or fraud threats by continually adding fraud detection tools.</td>
<td>Adding additional fraud tools without understanding how they work together could inadvertently undermine the effectiveness of the overall system and will often drive away frustrated applicants.</td>
<td>TransUnion Device Verification integrates with identity verification, allowing you to quickly approve new customers. This layer profiles user devices, device locations and device reputations. Combined with consumer information, this provides a comprehensive risk assessment—while remaining completely invisible to applicants.</td>
</tr>
<tr>
<td>Making decisions in isolation. (For example, verification and authentication processes are returned and analyzed separately.)</td>
<td>Multiple systems and multiple decision points often lead to costly piles of manual reviews. Problems happen when, for example, an applicant presents as low risk on verification but fails a three-question authentication exam.</td>
<td>TransUnion Authentication deploys an authentication routine and decides on complexity based on the combined verification/device assessment. By tailoring the complexity to consumer risk, good consumers are approved quickly and back-office reviews are reduced.</td>
</tr>
<tr>
<td>Building defenses that don’t change with time.</td>
<td>A one-size-fits-all approach can catch yesterday’s fraud, but leaves institutions exposed in a changing world. Difficulty adjusting strategy or integrating complementary new layers of defense slows your response, adds cost and contributes to lost revenue.</td>
<td>TransUnion ID Manager is an integrated product suite comprising identity verification, device verification and authentication modules. It lets you quickly—and confidently—approve low-risk customers and identify those who pose a true fraud risk. Built-in flexibility means you choose the modules you need now—and add capabilities or change strategies as your business changes and grows.</td>
</tr>
</tbody>
</table>

WHAT’S NEXT?

Find more resources at solutions.transunion.com/fraudprevention.

Contact your TransUnion representative or call us at 844-245-4071.