Onboarding New Customers Among a Host of Stolen and Synthetic Identities
Introduction

The digitalization of in-store services has resulted in a shift to online and digital-only experiences. At the same time, customers today expect seamless interactions at every step of their journey from new account creation to checkout. This has resulted in competing priorities for businesses including the need to rapidly innovate, enhance the customer experience, avoid disruption, meet evolving regulations, and reduce fraud.

Fueled by endless data breaches, new account fraud is at an all-time high as fraudsters have come to realize the long-term value of identity credentials over payment credentials. Unlike payment credentials which can be canceled immediately, identity credentials can be used to apply for a variety of credit and loans over a long period of time, enabling fraudsters to amass large amounts of debt before “busting out.”

This type of sophisticated fraud has added to the challenges faced by financial institutions – many of which still use legacy solutions that are unable to detect and block fraud that is based on real identity information.
New Account Creation Moves Online

Businesses have moved online to meet customer demand for convenience, ease-of-use, and faster service.

Establishing a new account provides entry into the walled garden of businesses, and customers and fraudsters alike seek access past this digital moat.

In the past, creating an account was an in-person, in-store experience, and an inconvenient one. However, as consumers and businesses have moved online, creating an account has become a predominantly data-driven, digital experience.

Account creation today is primarily data-driven. In-person trust has been replaced with a data-only approach to onboarding.
Increasing Fraud and Breaches – The New Normal

Data breaches have become all too commonplace in the digital-first economy. With an abundance of stolen credentials available for purchase on the dark web, along with detailed “how-to” instructions and “out-of-the-box” tools, cybercriminals have everything they need to orchestrate a variety of complex attacks on organizations across the globe.

Data breaches are fueling identity theft:

- **1579 breaches exposed**
  - **179M records**
- **44% more breaches**
  - **389% increase in records compromised**
- **$800M in losses for credit card issuers in 2017**

Manifestations of New Account Fraud

The main driver of application fraud is for criminal or financial gain through the fraudulent access to services such as loans and credit, or as a conduit for other financial crime, such as money laundering.

Identity Fraud can manifest in numerous ways:
• Applications using stolen identity information
• Applications using synthetic identity information
• Applications from customers using their own identity with the intent to commit fraud
• Applications from customers who are controlled by a crime group
The Impact of Bad Decisioning When Onboarding New Customers

New account creation is the first point of contact between a customer and an organization, and the first step in the customer journey. Halting fraudsters at this first step is not only imperative to protecting a business’ ecosystem, but also the most cost-effective way to prevent losses. Failing to block fraudsters at this first step can make it harder for businesses to detect and manage fraud later on in the customer journey, creating a host of problems, such as higher fraud losses, increased operational costs, and more regulatory scrutiny.

<table>
<thead>
<tr>
<th>Good Customer</th>
<th>APPROVE</th>
<th>DENY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase Revenue</td>
<td>Increase TLV</td>
<td>Decrease Revenue</td>
</tr>
<tr>
<td>Increase Acceptance Rate</td>
<td>Protect Brand Reputation</td>
<td>Decrease Acceptance Rate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bad Customer</th>
<th>APPROVE</th>
<th>DENY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase Revenue</td>
<td>Increase TLV</td>
<td>Decrease Revenue</td>
</tr>
<tr>
<td>Increase Acceptance Rate</td>
<td>Protect Brand Reputation</td>
<td>Decrease Acceptance Rate</td>
</tr>
</tbody>
</table>

The ultimate goal for businesses is to increase acceptance rates by allowing good customers to establish accounts while blocking bad actors. Failing to do so results in a host of problems.
Unpacking the Layers of Identity Fraud
Stolen Identities

Identity data has lasting value for fraudsters. With full profile identity data, fraudsters can pass a majority of checks against third-party validation services. Businesses relying solely on such services are left vulnerable to fraudsters armed with high-quality stolen identity data.

To maximize the potential of a full profile stolen identity, fraudsters make gradual changes over time in order to gain complete control of the identity. This might involve opening an account with the existing identity data, by altering the physical address, email, or phone number. Once onboarded, the fraudster establishes a good relationship with the organization by demonstrating responsible behavior, making purchases and paying off the balance each month.

Over time, credit is extended and fraudsters who often run the same scheme in parallel with multiple identities can easily amass hundreds of thousands in credit. Fraudsters then “bust out” by defaulting on all of the credit at once – leaving credit and lending companies with massive financial loss and a nightmare of a mess for their real victims.
Synthetic Identities

Synthetic identities are created by piecing together real and fictitious information to create brand-new identities.

Fraudsters establish credit histories for synthetic identities in the following ways:

- Multiple attempts to apply for credit creates a “thin file” with credit reporting agencies (CRAs) and eventually a lender grants a low line of credit.
- “Piggybacking” a legitimate cardholder’s account results in a synthetic identity inheriting the cardholder’s credit history after a short period of time.
- Fabricating a history of credit payments for a synthetic identity by exploiting the relationship between a business and CRA through the use of a front company or insiders at a legitimate business.

Once credit has been established for a synthetic identity, it can be used in the same way that a stolen identity can – to apply for a range of credit and lending accounts, such as car loans, credit cards, personal loans, mortgages, and more. However, the challenge for businesses is that when a fraudster uses a synthetic identity versus a stolen identity to apply for loans and credit, they are sent down a rabbit hole, attempting to reclaim debt from a person who never existed.
**Synthetic ID Factories**

Fraudsters exploit loopholes in the way credit reporting agencies update credit files to industrialize the creation of synthetic identities with strong credit histories.

- **Data Breaches**
  - Child or Deceased SSN (valid but unused)
  - Valid Name and Address, Name and DOB, Name and Phone etc combinations

- **Dark Web Marketplace**

- **CRA check No File**
- **Apply for low level credit**
- **New Synthetic ID**
- **“PiggyBack” existing credit file**
- **Add “authorized user” for several days**
- **CRA passes credit history to new “authorized user”**

- **CRA creates File**
- **Good Credit Rating**
- **Repeat until successful**
- **Make regular repayments**

New identity that passes identity checks and has a good credit history.
Businesses Need A Layered Defense

Building a layered defense is the key to identifying and blocking account applications using stolen and synthetic identity credentials in order to increase acceptance rates.

By combining various static and dynamic data sources with powerful machine learning, organizations can obtain actionable insights to help protect themselves from evolving fraud, while also providing a frictionless experience for legitimate customers and addressing changing regulatory requirements.
The Simility Solution for New Account Fraud includes all of the components needed to help protect an organization from application fraud and is designed to improve acceptance rates.
The Simility Solution for New Account Fraud

Simility, a PayPal service, offers an end-to-end fraud and decisioning platform built with a data-first approach to provide a 360-degree view of the end user, designed to protect the customer journey. The Simility platform incorporates dedicated services to help organizations detect new account application fraud and uncover the use of stolen and synthetic identities.

The Simility Solution for New Account Fraud includes:

- Built-in device and session forensic collectors via Javascript, iOS and Android SDKs.
- A flexible API with a pre-built, but extensible, schema for receiving new application data and back filling historic data and fraud label data.
- An out-of-the-box and extensible data processing pipeline that automatically joins data across multiple data sources including fuzzy matching on physical addresses and email addresses.
- An out-of-the-box integration with key third party APIs to augment identity validation and cross referencing including CRA data and alternative consortium data sources.
- A UI driven rules engine with out-of-the-box detection scenarios for immediate benefit. New rule suggestions and rule re-weightings are automatically suggested by an in-built machine learning model that continuously improves from the fraud label feedback.
- A pre-configured, tree-based machine learning model, that runs in parallel to the rules engine, with advanced machine learning interpretability algorithms. The model can be re-trained and tuned on the available historical fraud label data. Additional models and extensions can also be applied with support for Champion-Challenger evaluation.
- A UI driven decision layer that takes output from the rules engine and the ML model and enables organizations to finely control accept, review and reject rates.
- An alert management and investigation interface with pre-configured workflows for rapid evaluation of review cases. This includes a simple view of the application and the key identified risks, as well as the ability to drill down to related applications and also full link visualization and exploration to detect complex fraud rings. This view can be extended with options such as geo-mapping of address versus IP locations and other useful visual indicators.
- A performance and alert management interface based on key performance indicators.
Conclusion

While data breaches are far from over and the threat of identity related fraud continues to grow, it is possible to leverage the advanced capabilities of Simility’s Adaptive Decisioning Platform to stay ahead of sophisticated and evolving fraud.

Simility helps enable financial institutions to protect their ecosystem by automatically detecting emerging fraud patterns in real time before they become a problem, and designs solutions to reduce friction for legitimate customers during the onboarding process – thereby helping to improve overall acceptance rates.
ABOUT SIMILITY

Simility, a PayPal service, offers real-time risk and fraud decisioning solutions to protect global digital businesses. Simility’s offerings are underpinned by the Adaptive Decisioning Platform built with a data-first approach to deliver continuous risk assurance. By combining artificial intelligence and big-data analytics, Simility helps businesses orchestrate complex decisions to reduce friction, improve trust, and solve complex fraud problems. Built by industry veterans, Simility is trusted by some of the world’s leading consumer brands across financial services, payment processors and commerce merchants. For more information on Simility, visit Simility.com