Accertify
AN AMERICAN EXPRESS COMPANY

Get Ahead in the Fight Against Digital Account Opening Fraud

BEST PRACTICES FOR REDUCING DIGITAL ACCOUNT OPENING FRAUD

Best Practices for Reducing Digital Account Opening Fraud

As our world becomes more digital, so too does banking. While services like viewing your balance or making a payment has been the norm for many years, the ability to open an account digitally lagged behind. Currently, only 56% of financial institutions allow digital account opening[1], but that number is expected to increase as more banks and credit lenders meet the expectations of their customers and also adapt to the digital acceleration that has resulted from the COVID-19 pandemic.

While digital account opening has many advantages, like a significant decrease in onboarding costs and the ability to cater to customers' schedules, it also introduces the risk of fraud. The ability to detect and prevent digital account opening fraud, specifically synthetic identity fraud, has made it difficult for many financial institutions to offer online account opening to their customers.

However, to remain competitive, many banks, credit unions, and other credit issuers must balance delivering a differentiated customer experience with the appropriate fraud controls. While there is not a silver bullet, fortunately, the tools, technologies, and solutions have matured to help detect and prevent digital account opening fraud. But first, let's explore the potential fraud threats with online account opening and then understand the best ways to mitigate those risks.

[1] https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/financial-services/ce-digital-banking-maturity-2020.pdf

FACELESS FRAUD

Criminals may purchase personally identifiable information on the dark web, normally resulting from a data breach, or they may "steal" a victim's identity, many times through social engineering tactics like phishing, smishing, and vishing to create a synthetic identity. They then use that synthetic identity to open a bank account, apply for a credit card, or establish a line of credit.

Perpetrators then nurture the accounts for many, many months or even years – paying the balance each month – to build up their credit history with the financial institution. At this point they will strike, typically referred to as bust-out fraud, and leave the creditor to write off the debt and deduce what happened.

WHAT IS CAUSING A RISE IN SYNTHETIC IDENTITY FRAUD?

This rise of synthetic identity fraud allows cybercriminals to commit digital account opening fraud more easily. Here's why:

1. WITH SYNTHETIC IDENTITY FRAUD, THERE IS NO "REAL" VICTIM TO REPORT THE CRIME. PERPETRATORS CAN OPEN AND DEFRAUD NUMEROUS ACCOUNTS WITHOUT ANYONE RAISING THE ALARM.

2. DUE TO THE NUMBER OF DATA BREACHES AND SECURITY COMPROMISES, IT IS INEXPENSIVE TO PURCHASE A SOCIAL SECURITY NUMBER – THE SCAM'S CORNERSTONE – ON THE DARK WEB.

3. BEGINNING IN JUNE 2011, THE U.S. RANDOMIZED HOW SOCIAL SECURITY NUMBERS ARE ISSUED. CONSEQUENTLY, BANKS CAN NO LONGER USE NUMBERING CONVENTIONS FOR CROSS-CHECKING APPLICANTS' PLACE OF BIRTH, AGE, OR OTHER INFORMATION.

Typical third-party fraud controls, like sending a one-time passcode for second factor authentication or prompting the applicant to answer knowledge-based authentication questions no longer apply because the criminal is in possession of all this information.

FIGHTING BACK: KEEP THE OLD, ADD THE NEW

Cybercriminals are continuously developing new and improved ways to commit digital account opening fraud. As a result, financial institutions need to remain vigilant, balancing both new technology and investments with traditional measures and controls. Some legacy processes that may transition into the online world and prove effective include:

Request applicant to upload documents. While this may introduce unwanted friction and add time to the process, new services have emerged to verify a document image for authenticity.

Consent Based Social Security Number Verification. The Social Security Administration (SSA) is currently developing a new electronic Consent Based Social Security Number Verification (eCBSV) system, which will allow permitted entities to accept electronic consents. This may restore some of the advantages lost when SSN randomization was introduced, but limited matching capabilities may be problematic or potentially introduce false positives.

While these methods may uncover some attempts to commit digital account opening fraud, they primarily rely on processes that impede the customer experience and may lead to abandonment or not scale to meet desired service levels.

HOW DO LEGITIMATE USERS BEHAVE?

As the evolution of account opening fraud outpaces most legacy processes and systems designed to detect it, financial institutions, especially smaller ones, need to continue to invest in software platforms that lead with machine learning, enable consortium data sharing, and expore new technologies. One that has shown promise is **behaviorial biometrics,** which can provide rich analytics and crucial insights into online customer activities and intent. Behavorial biometrics, sometimes also referred to as user behavior analytics, can detect account opening attempts that deviate from legitimate users' patterns, including keystroke dynamics, page navigation, and mouse and cursor movements. These "intent" signals can be captured in real-time and flag which account activities require further investigation and authentication, helping to remove some of the manual review burdens.

When you marry the combination of explainable machine learning, consortium data, device intelligence, and behaviorial biometrics, millions of data points can be compared across industries, devices, and account types, allowing banks and other financial institutions to assess risk and design and develop protocols on how to handle the various risk levels. **This is the backbone of Accertify Digital Identity.**

Enable genuine applicants to receive an optimal customer experience and proceed with little to no friction at all. At the same time, mitigate risk when suspicious patterns and attack vectors arise.

Accertify
AN AMERICAN EXPRESS COMPANY

REQUEST A CONSULTATION

to learn how Accertify Digital Identity can provide a multi-layer defense against account opening fraud.

Trust Accertify.

accertify.com