There is no question that 2020 silenced any lingering doubts regarding the need for businesses interested in staying in business to embrace digital transformation.

While the digital mandate is not new, COVID-19 has brought it into sharp focus. Indeed, one of the most material effects of this is the revolution in how we pay for goods and services. As more consumers worldwide have begun shopping online since the declaration of the pandemic in March of 2020, data from IBM’s U.S. Retail Index predicts an accelerated shift to e-commerce by five years.

Moreover, nine-year-old video communication software provider Zoom is now worth more than Exxon Mobil, the oil giant that can trace its founding back to John D. Rockefeller’s 1870 formation of Standard Oil. The times? They are a-changin’!

For traditional banks to keep up and keep their customers in tomorrow’s digital economy, they need to understand the value of detecting fraudulent behavior early and accurately while maintaining a frictionless experience for their customers.

Let’s investigate.
The Competitors

Given the impact that COVID-19 is having on the global population, there is now a growing belief that a new digital model of banking will play a critical role in addressing the shortcomings posed by traditional lenders.

A neobank is a type of bank that has no physical branch network or legacy infrastructure, operating exclusively through digital channels. This means that all business conducted with a neobank is through digital means, such as online platforms and mobile apps.

A challenger bank is an established firm that operates with a full banking license in the market. Typically, these banks offer a much broader suite of financial products and services such as lending, investments, and savings, checking and merchant accounts, credit cards, trade products and more.

Together, neobanks and challenger banks are continuously challenging traditional lenders by innovating several technologies and integrating in their product offerings. They have seamlessly entered the market with advanced features, real-time services, and customer-centric products and services.

According to a Global Opportunity Analysis and Industry Forecast into the Neo and Challenger Bank Market, the global industry was valued at $20.4 billion in 2019 and is projected to reach $471.0 billion by 2027, growing at a compound annual growth rate of 48.1%. In fact, a recent study conducted by research company Censuswise on behalf of digital banking fintech company Crealogix estimates that one in every four people under the age of 37 in Western Europe currently uses a digital bank.

The (neo and challenger bank) global industry was valued at $20.4 billion in 2019 and is projected to reach $471.0 billion by 2027, growing at a compound annual growth rate of 48.1%.

Meanwhile, in Switzerland, arguably one of the world’s most advanced nations for banking, an annual study jointly conducted by the ZHAW (University of Applied Sciences Zurich) School of Management and Law and the University of St. Gallen, one-tenth of 1,200 Swiss residents surveyed at the end of 2019 had already used new online-banking solutions provided by challenger and neobanks.

Perhaps the biggest growth opportunity for neobanks is actually in the developing world and emerging economies, where such digital
Account Opening & Fraud Prevention

The trend to open new accounts through online digital channels rather than in-branch openings actually started in 2019 and has, no doubt accelerated by COVID-10, continued in 2020, with the volume of digital account openings up 66% YOY in 2020.

This is a serious adjustment for many traditional banks! A customer walking into your local branch to open an account or apply for a loan in person was ideal in that it provided a clear form of identity security and trust for both the customer and the bank.

Now, banks need to provide that secure, frictionless customer experience digitally. And this means focusing on step one: opening an account. While in the past, many Fraud Managers might focus on a fraudulent transaction after the fact, in today’s digital economy, it’s too late.

Synthetic identity fraud is the fastest growing crime in the world and costs lenders an estimated $6 billion every year. This sophisticated type of theft is where a bad actor uses the personal information of different people to create an authentic-looking...
identity. One of the most common uses of synthetic identities is to commit account opening fraud. Indeed, this is the onset to a slew of opportunities waiting to be exploited by a fraudster who is one step ahead! From establishing a bank account to preparing for loan applications or money laundering to creating online accounts for fraudulent transactions, fraudsters are clever and creative in how they make use of the system.

One of the largest synthetic identity fraud schemes recorded led to confirmed losses for businesses and financial institutions totaling more than $200 million. The scammers fabricated more than 7,000 false identities, which were used to obtain thousands of credit cards.

Let’s face it. Often, the real victim of synthetic identity fraud is the financial institution. According to Equifax, it accounts for 80% of all credit card fraud losses, and nearly one-fifth of credit card charge-offs - and that was pre-pandemic!

Early and fast fraud detection is key. To mitigate losses, banks need to leverage technologies such as machine learning and artificial intelligence to replace the traditional face-to-face identity confirmation of live in-person banking. By investing in an innovative solution uniquely tailored to issues related to account opening, banks can streamline the onboarding experience for good customers while simultaneously enabling identification of fraudsters.
RISK MANAGEMENT:

Credit Risk or Fraud Risk?

If customers are now banking online, how do banks know they are whom they say they are? How do they assess the bad actors? Traditionally, banks have relied on the deterministic data associated with regulated credit risk management. The bank was able to specifically identify a potential customer through a combination of static identity elements such as national ID, date-of-birth, address, and biometrics – the standard physical know-your-customer processes.

While this was all well and good in face-to-face situations, as banking digitizes, businesses will be required to rely on more of a probabilistic approach in order to determine fraud risk. Simply put, while deterministic data has long been considered the gold-standard in identity verification, it inherently involves too much friction. Moreover, assessing credit risk with deterministic reasoning does not account for account takeover or stolen identities.

Meanwhile, the increasing accuracy of probabilistic data tracking associated with fraud risk is great news for banks forward-thinking enough to invest in machine learning technology to combat criminal deception.

Indeed, given our understanding of the limits of static personally identifiable information, the dynamic identity elements required in fraud risk assessments (phone numbers, email addresses, device IP, etc.) allows financial institutions to be flexible; to shift, expand, loosen or contract based on their needs at the time.
What all banks need is to partner with a data provider who can answer: Is this customer legitimate or are they an actor?

To build a strong bank fraud detection strategy, financial institutions need comprehensive analytics. Advanced analytics software provides the tools necessary for banks to recognize and act on suspicious patterns, quickly notify customers of fraud incidents and position themselves for faster settlements.

In some countries, new regulations are insisting that banks open an application programming interface (API) so that they can ensure greater interoperability, allow for greater consumer control over financial data, diversify the range of products available to customers, and, of course, enhance competition. Meanwhile, banks in other countries see the potential of creating a platform approach and are taking the initiative by opening APIs and integrating with new partners. What all banks need is to partner with a data provider who can answer: Is this customer legitimate or are they an actor?

“In assessing fraud risk, there is no legal definition of trusted data, no regulated trusted source,” explains Ekata’s CEO Rob Eleveld. Instead, the onus is on the data vendor and how seriously they take data.
“(At Ekata) we only use data that our data vendor has the right to license,” continues Rob. “We want to know where they got it. We use a personal touch; traveling to our global data sources, meeting with our vendors around the world. We spend a lot of time on trust, vendor by vendor.”

We spend a lot of time on trust, vendor by vendor.

Like all Ekata products, our Account Opening API is powered by the Ekata Identity Engine. This engine consists of two main components - the Identity Graph and the Identity Network. The former takes into account five data inputs: name, phone, address, email, and IP address, and helps validate the digital identity elements and how they are linked. The Identity Network analyzes how these identity elements are being used.
This signal is designed to capture the frequency of an IP address being seen on the platform. The most recent address usually bears higher risk than one seen months earlier. While it is not common for a good customer to create multiple bank accounts in a short period of time, a fraudster may be more inclined to cluster fraudulent account creations using proxy IPs or public WIFI.

Unlike the previous two signals, this signal does not show when the identity elements were last seen but rather when they were first seen together. In the instances where fraudsters try to use disposable or temporary email and phones, this combined signal helps capture them. Because they are created recently and change frequently, the longevity of the elements seen together could mean that they may be of lower risk.
Of course, while fraud detection needs to be at front of mind for any financial institution, customers still need to be unfettered by friction. According to VansonBourne Research into the Infinite Want of Consumers,

“Added security (for customers) needs to be ‘behind the scenes,’ through smart use of emerging technologies and methods such as machine learning and intelligent risk modelling… (that) enable companies to quickly and stealthily review for fraud, while leaving the customer experience untouched.”

By implementing a sound risk assessment strategy in onboarding customers, banks can tailor an equally seamless and trusting online application experience. This will go a long way in alleviating any fear a customer may have in establishing an account and putting their life savings into it. At the same time, such an implementation would fight the fraudsters with stolen and synthetic identities trying to get onto the platform.

Good Customers Deserve a Good Experience

WHAT’S NEXT?

Making the Change

So, where to from here? Here’s hoping your boss sold his Exxon stock before the pandemic hit, but let’s face it; no one saw this coming. Now that we know the world is changing faster than ever predicted, you can still come out on top. Appreciating where the banking competition is heading and preparing your digital offerings accordingly is a solid step. Understanding the pros and cons to credit risk and fraud risk is another. Most importantly, partnering with a data provider who takes their analytics seriously is vital.

Contact Ekata today for a historical data test, and let’s take it from there.
Sources


