WHITE PAPER

DIGITAL ONBOARDING IN THE POST-PANDEMIC NEW NORM

CONSUMER LENDING

CARD ISSUING

ONLINE BANKING

ECOMMERCE

NEURO-ID®

HUMAN ANALYTICS™ FOR THE DIGITAL WORLD

neuro-id.com

TABLE OF CONTENTS

INTRO

In the first quarter of 2020 the U.S. economy came to a screeching halt. Tens of millions lost their jobs while the unemployment rate increased more than five-fold. This sent ripple effects through the entire economy as consumers and businesses scrambled for liquidity and struggled to make ends meet. Meanwhile, some industries underwent a digital transformation seemingly overnight as consumers instantaneously migrated to digital channels to avoid spread and exposure to COVID-19.

Fraudsters saw the pandemic as an opportunity. They exploited consumer fears with phishing attacks, targeted those working from home where network security and best practices lacked, and increased fraudulent orders and loan attempts, often with these freshly stolen identity data and credentials, against organizations who couldn't even keep up with the increase in legitimate demand. Businesses with a digital presence were fighting a war on multiple fronts.

The multitude of impacts resulting from COVID-19 didn't just occur rapidly, they also showed longevity. Consumers formed new habits that will stick while businesses continue to utilize the investments and infrastructure in digital channels they quickly brought to fruition.

THE NEW NORMAL IN DIGITAL ONBOARDING

Nearly everyone in the world was impacted, indirectly if not directly, by COVID-19. The focus of this document is to discuss the impacts specific to onboarding consumers or businesses in digital channels across six different industries. While there are specific pain points and nuances to each of these industries, **there are also fundamental truths that impact digital onboarding during and post the pandemic**.

1

First is that fraudsters never let a crisis go to waste. Whether a consumer was desperate for essential supplies, a speculative cure or new employment opportunities, they were an even easier-than-usual mark. Whether a business was forced to quickly increase their digital presence or was simply overwhelmed by the increase in online demand, they were unsympathetically targeted with attacks. The confluence of higher availability of freshly stolen identity information and an opportune time to attack businesses already under duress was the professional fraudster's dream.

Many organizations turned up the fraud controls as a result. This, coupled with changing consumer patterns that made normal-risk customers or applicants look more like higher-risk ones, led to a significant spike in false positives. **Credit and risk modeling systems that used to work adequately, suddenly broke down**.

2

Second was the overnight change in what consumers needed to make ends meet and the level of creditworthiness they now represented, that was somewhat unmeasurable for most organizations. Stimulus checks came quicker for some than others, but never as quickly as people lost their employment or were furloughed. State unemployment systems hit backlogs and failed to provide many with their benefits for weeks to months. Consumer reactions to their sudden drop in income manifested in many different ways. For some this meant applying for uncollateralized loans or more credit cards. For others it meant deferring to pay rents or revolving credit debts. For some it meant fighting every credit card charge they had a chance to win, regardless of whether the claim was honest.

Traditional credit reporting methods were suddenly of much less significance. People with pristine credit could be out of work and income. People may have applied for multiple loans and credit cards in a very short amount of time. People who fit the mold of a genuinely good borrower based on strong credit history and low level of outstanding debt as of last month could be in an entirely different state of financial standing at the time they were applying or onboarding. Due to time and reporting lags, traditional credit reporting methods could not keep pace with the rapid rate of unemployment and new level of consumer credit outstanding. Past performance is not a guarantee of future success, and that's true now more than ever.

How should organizations adapt to these new challenges when it comes to onboarding new applicants?

Rely less on the PAST and more on the NOW. Cultivate signals and data with less of a time and reporting lag to supplement those which had a sudden fall in predictive accuracy. Organizations who were able to focus more on behavioral signals, which solve or are immune to the time lag and model breakdown issues, were much better equipped to detect potential first- and third-party fraud during the pandemic and continue to benefit from these techniques and signals.

CONSUMER LENDING

Digital Events & Pain Points

Consumer lending and uncollateralized loans have been prevalent in the digital channel for some time. What changed in 2020 was the **volume of applicants**, their **default risk** and the risk of issuing unrecoverable loans to **identity fraudsters**.

Onboarding is the first step of the loan application process. In the digital channel this requires collecting and validating identity information, then moving on to income validation and credit checks after building confidence that the identity is authentic and actually the person you are dealing with on the other side of the screen.

The problems that arose due to COVID-19 were threefold. First, that synthetic identity fraud and stolen identities were being used in fraudulent loan applications more frequently. Second is that even when an applicant was who they claimed to be, gauging their default potential was much murkier than before. Reasons for this ranged from applicants being dishonest about their financial and employment status to increase the likelihood of loan approval, to traditional credit reporting methods not being able to keep pace with the rate of change in a consumer's financial standing. The third issue is that enforcing identity checks and navigating new methods to determine creditworthiness isn't an excuse for destroying the user experience. Seeking balance is always important, but now more difficult than ever before.

As identity fraud checks are typically lower cost than credit checks, it is prudent to weed out the synthetic and untrusted identities first. This doesn't focus solely on the identity data, but also by looking for repeat patterns and activity that is indicative of bots or automation. Behavioral signals can provide substantial benefit in detecting automated and repeat activity even as sophisticated fraud rings present new, clean identities and effectively spoof their devices.

What may have become most difficult is the ability to recognize applicants committing first-party fraud, providing inaccurate information, even when traditional credit reporting data said they were reliable. Even people with a strong credit history can represent an elevated potential for default if we do not understand their current financial situation. Someone could provide an image of a pay stub from two weeks ago, but it does not guarantee they still have that job at the time of their loan application.

Alleviating the Pain

When it comes to validating financial and identity information, maintaining a low-friction user experience for the onboarding process is still important. This means supporting mobile picture uploads and abilities to take and provide pictures of an ID and paystub within a mobile app or mobile application process. Services that allow consumers to take a photo of their ID for identity verification (KYC checks) but also auto-populate the onboarding application go a long way in maintaining convenience and minimizing the time to complete an application.

The challenges around identity authentication and verification were not new, just needed to catch the more frequent attempts at using stolen or synthetic identities. The most pressing challenge in the consumer lending space became getting an accurate picture of an applicant's credit and default potential.

COVID-19 reduced the value of traditional credit reporting data and for lenders this meant focusing more on the now and less on the past. Behavioral analysis plays an important role here, especially when there is a cognitive component.

When a banker interviews a small business or personal loan applicant, they ask questions and pick up on non-verbal cues. Noting whether the applicant maintained eye contact, showed any physical signs of being nervous or anxious and other "tells" can tip off the lending agent when the applicant may be less forthright. Neuro-ID is the only solution that provides a way to recreate this in the digital channel.

Neuro-ID clients, both old and new, have been able to leverage such behavioral and confidence signals by asking applicants targeted questions that could fit into existing loan application questionnaires.

These questions focused on the recent events to derive signals too new to show up in any traditional or alternative credit reporting data. Examples include:

- *Have you filed for unemployment benefits in the past 90 days?*
- *Have you been furloughed from your job?*
- *Have you recently experienced a reduction in employment hours per day?*

A pandemic-triggered shift in behavior patterns

Analyzing Neuro-ID client data and leveraging unique data insights, we can see the massive shift in consumer and loan application patterns. Once the pandemic and lock down orders hit, there was a significant drop in daily loan application interactive volume, but this is was accompanied by a three-fold spike in input field interactions that an applicant changed or altered at some point during the online application process specifically for the Employer Name and Income fields. Whereas 13 to 14 percent of loan applications would see the applicant revise their reported income or employment information pre-pandemic, this increased to 45 percent of applications during the pandemic.

This excessive manipulation of employment and income fields is highly correlated with first party fraud or Intent Fraud, where someone intentionally misrepresents information to achieve a more favorable outcome. Lenders leveraging Neuro-ID's proprietary technology were able to uncover these anomalies, while those relying only on credit reporting and income verification measures couldn't see how many applicants were reporting employment that has been furloughed or lost.

Fig 1.0 - Increase in anomalous behavior with 'employment' and 'income' fields, indicative of first party fraud

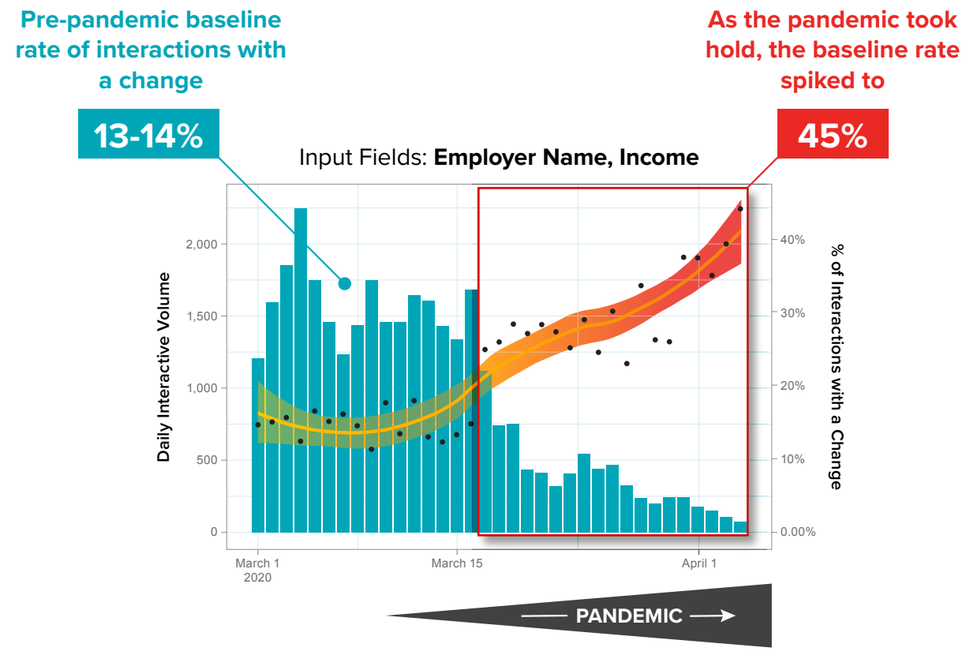
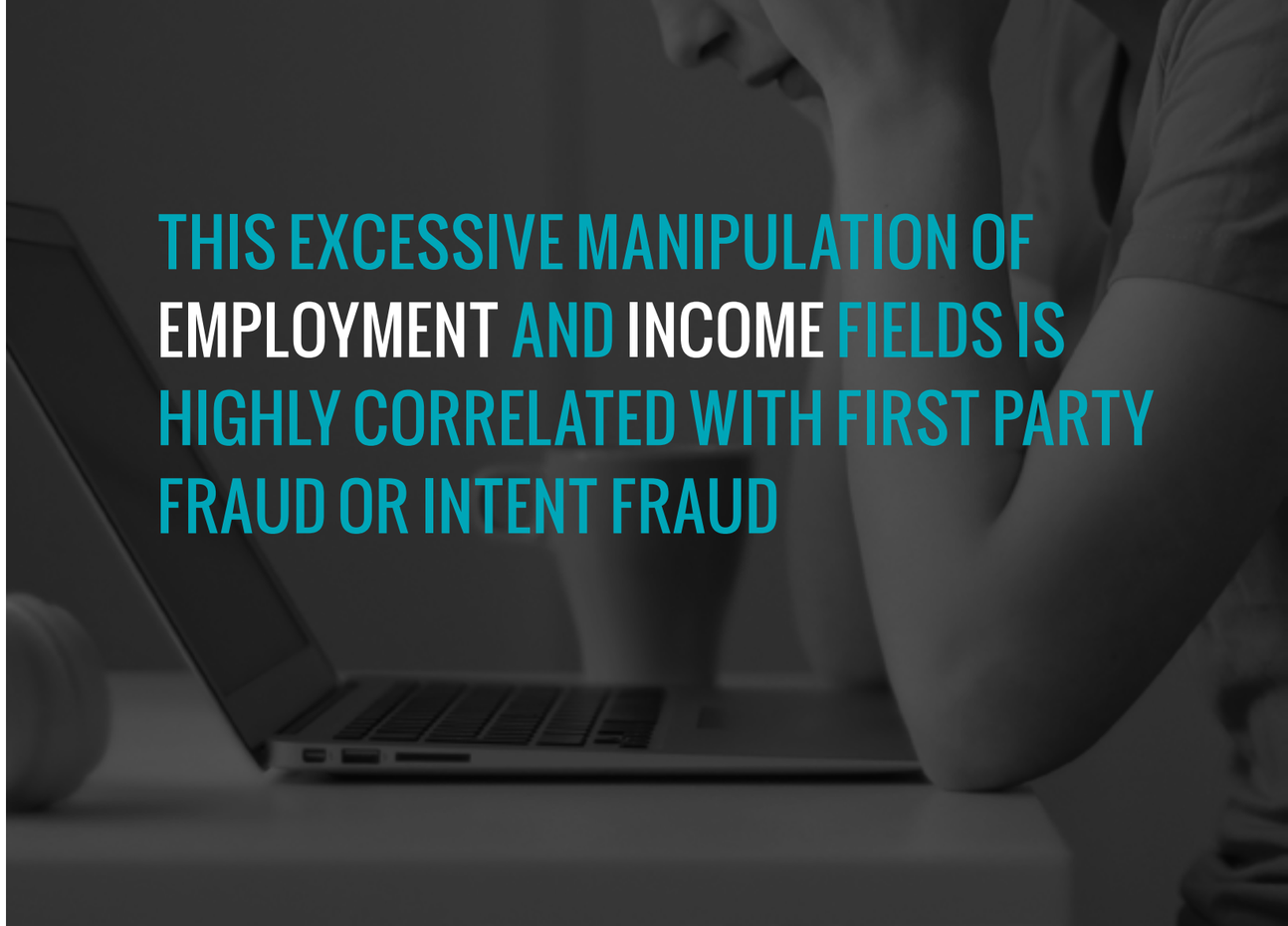


Figure 1.0 - Based on population of 606,035 application sessions across the Payments industry, from March 1 through April 4, 2020



CARD ISSUING

Digital Events & Pain Points

Credit card offers and applications by mail came to an abrupt stop while more consumers tried to increase credit limits or apply for new cards and were funneled to digital channels to do so. **This put additional strain on card issuing banks** that now had to review more credit card applications while fraud and credit analysts transitioned to work remotely.

Large card issuers have facilitated online applications for years, but regional banks and credit unions may not have offered the same level of features. While banks were deemed essential, consumers still did not want to visit a branch to take out a new credit card, and many issuers rushed to new or white labeled online systems for accepting credit card applications.

The increase in credit card applications included fraudulent applications with stolen identities and legitimate applications with compromised and questionable credit. Many consumers planned ahead by applying for new credit cards while they were able to pay off existing balances with stimulus checks, knowing they'd need the increased lines of credit in the future when the stimulus funds ran out before they might resume full-employment.

Just as with consumer uncollateralized loans, consumers wanted to paint a rosier picture of their financial status while traditional and alternative credit reporting data has too much of a lag time to keep up with the changes in debt and employment that may have occurred in the most recent weeks or days.

Consumers applying for credit cards can have higher potential for default than those who applied for direct loans. They are willing to take on a higher interest rate with credit cards compared to uncollateralized loans, often because their personal loan applications may not have been approved. Many consumers stacked loans and new credit cards applying for multiple new lines of credit in the same day. This loan and card stacking does not appear in credit reporting data instantaneously.

The response of most card issuers, which was unfortunate for both the issuer and consumers, was simply to stop or greatly reduce the number of new credit cards issued.

Alleviating the Pain

Focusing on the *now* and the most current events is the best way to understand the current level of risk a given card applicant represents. This is the only way to identify loan stacking, multiple credit card applications across different issuers and recent loss of employment which could be temporary or permanent.

Effectively assessing and managing credit risk not only requires understanding the now, but also understanding the risks in the near- to intermediate-term future. Those furloughed or possibly now structurally unemployed may only be in decent financial standing at the time of application because of the use of stimulus and additional Federal unemployment benefits, which won't last forever.

What happens when that runs out?

Gaining insight here is nearly impossible without a behavioral confidence indicator like Neuro-ID.

Card issuers most equipped to measure and assess their true credit and card default potential were able to fit new, highly targeted questions into their online credit card applications. This included examples such as:

- *Do you have other credit cards with a past-due balance?*
- *How many other credit cards do you currently have?*
- *Do you plan to use this credit card for cash withdrawals or advances?*
- *How many credit card applications have you completed in the last 30 days?*
- *Are you currently paying off debt on other credit cards with a consolidated loan?*
- *Have you been furloughed or laid off in response to COVID-19?*
- *Have you already received and spent all of the stimulus money provided as part of the CARES Act?*

This isn't simply about asking the right questions, but also *having confidence in the response*. Neuro-ID's technology and solution can reveal the intent of the applicant, leveraging real-time behavioral analysis and providing an unmatched level of actionable intelligence.

ONLINE BANKING - SAVINGS & DEPOSITS ACCOUNTS

Digital Events & Pain Points

Whereas lenders and card issuers had to increase scrutiny around and find more ways to assess a consumer's default risk, depository financial institutions faced a different set of challenges. This included **screening new account holders and performing KYC checks entirely online**, while being **careful not to aggravate and potentially lose new accounts**, many of which could become "whale" banking clients.

Whereas lending and card issuing problems revolved around the potential for direct loss from fraudulent loans and those that will end in default, the problems around onboarding new deposit account banking clients in digital channels centered around maintaining a strong user experience for the onboarding event while still keeping fraud and money laundering at bay.

The stock market bottomed in late March 2020, but smart money withdrew a large share of their equity holdings before then. Suddenly people were sitting on more cash than ever before, and most were in no rush to put that money back to work until they felt confident enough to do so. At the same time, potential debt and solvency issues for businesses and consumers seemed like a risk to threaten financial institutions. Those managing their assets know the Federal Deposit Insurance Corporation (FDIC) protects their checking and savings deposit, but only up to $250,000 held at each bank.

The response was to open more bank accounts. Any amount above $250,000 deposited at one financial institution is unrecoverable if that bank fails, so those with such levels of wealth spread their money to new financial institutions to take advantage of this Federal deposit insurance.

This is the textbook definition of a "whale" client, one with extensive wealth who, if you impress, can be retained as a client beyond the crisis at hand, and potentially stealing them away from competitors. Onboarding these clients, however, presents a unique set of challenges.

These new prospective banking clients may be opening accounts with large sums of cash, possibly even the max-insured FDIC amount, a quarter million dollars. This will raise red flags. All KYC, Due Diligence and AML checks must be performed and there must be a high degree of certainty that the prospective client is who they claim to be.

On one hand, you really don't want to offend and lose this prospect. On the other, you have to consider the possibility of clean fraud or the use of a stolen complete identity as a means to launder money or hide ill-gotten gains until they can be transferred elsewhere.

From the "whale" client's perspective, they are a valuable customer and should receive preferential treatment. A multi-day onboarding verification process isn't going to cut it. The challenge is balancing their expectations and pulling out every stop to win them as a client, not just in the short run but permanently, while still meeting all compliance and risk requirements.

Alleviating the Pain

This issue boils down to determining whether a new prospective banking client is a "whale" or a money laundering criminal ring. While KYC and AML checks need to remain in full force, there are additional qualitative signals that can ease concern and support a quicker onboarding process.

You have one chance to make a good first impression when digitally onboarding a new consumer. The strength of Neuro-ID's proprietary technology and platform is not just the ability to detect potential fraud, but also the ability to inform verification to decrease friction. Previous examples discussed uncovering an applicant's intent to inform verification measures around fraud, but when they show signs of complete honesty and transparency, these applicants can be fast-tracked and set to onboard on the path of least resistance.

Banks can gleen key insight by adding a behavioral layer into their existing processes

Here is how Neuro-ID can be positioned to support this within an existing digital onboarding environment for bank deposit account opening and onboarding:

- *What is the source of the funds you are using to open this account? (Sale of Equities, Sale of Real Estate, Cash moved from another bank, etc.)*
- *Do all funds used to open and later deposit into this account belong to you?*
- *Are you an agent managing fiduciary duties on behalf of another person or organization?*

Behaviors reveal a clear uptick in fraudulent activity

Again leveraging Neuro-ID unique data insights and client data, we analyzed what changed during the pandemic. At the application onboarding stage across multiple industries, seeing anomalous entry into identity input fields like name and email address is correlated with identity fraud and third-party fraud. Catching this behavior upfront allows organizations to more heavily scrutinize applicants showing these high risk signals via step-up authentication measures or manual review, while fast-tracking those with low risk signals through a smoother onboarding process with less friction.

Gauging familiarity with the form, an indication of whether the user has completed this same onboarding process before, as well as typing fluency, characteristics of automated and systematic or repeated entry methods are detected. Applications and onboarding volumes were higher before the pandemic and, on average, about 0.25 percent of onboarding events showed these onboarding familiarities or automated entry signals. During the pandemic this increased four times over to 1 percent of onboarding events.

For financial institutions who want to welcome new clients during a difficult time, being able to weed out those showing identity fraud and repeat onboarding signals is an asset that allows the recognition of these high risk signals to step-up authentication on these users, while offering a lower friction path to those who can be identified as lower risk.

Fig 2.0 - Increase in anomalous behaviors with 'identity' fields, indicative of third party fraud

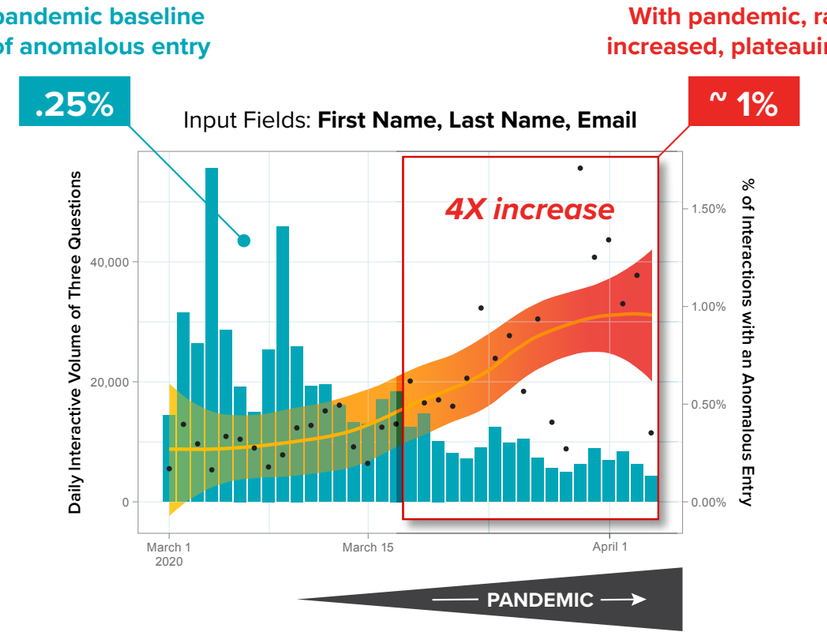


Figure 2.0 - Based on population of 606,035 application sessions across the Payments industry, from March 1 through April 4, 2020

SEEING ANOMALOUS ENTRY INTO IDENTITY INPUT FIELDS LIKE NAME AND EMAIL ADDRESS IS CORRELATED WITH IDENTITY FRAUD AND THIRD-PARTY FRAUD

E-COMMERCE RETAIL: CONSUMER ACCOUNT & LOYALTY PROGRAMS

Digital Events & Pain Points

Online fraud grew during the Great Recession of 2008 and 2009 including third party fraud and “friendly” or first party fraud. As consumers endure large declines in income and loss of employment, many seek to recoup money anyway they can. For some this means filing **false disputes or chargebacks** and for others it means finding ways to **abuse or take advantage of incentive offers and loyalty programs**.

It isn’t difficult to create a new, free email. Merchants need to be on the lookout for users who create multiple accounts to continue to use free-trial periods or claim first-time customer offers, which can often provide a good or service at break-even or a loss.

Another common pain point for merchants is loyalty program abuse. Loyalty programs are important as they cultivate customer retention, repeat buyers and stickiness, but if not managed properly they can come at a cost. Customers will make purchases to build up points then request refunds. They will also refer themselves or fake accounts to join an email list or make a purchase if it comes with an incentive. Incentives often create unintended consequences which are difficult to foresee, but eventually consumers will find a way to exploit them.

Customer loyalty programs can encourage consumers to leave a merchant for their competitor. When selling in a competitive market it is important to offer incentives that increase repeat buying activity and turning off loyalty programs or reducing their incentives in response to fraud or abuse is not ideal.

Alleviating the Pain

Managing loyalty programs is about keeping consumers honest, and that can be more difficult in a digital environment. Neuro-ID can provide valuable signals at the onboarding stage of creating a loyalty account, whether that is a new loyalty account or one that was referred in response to some incentive.

Cultivating new signals of risk leveraging Neuro-ID’s behavioral signals involves detecting anomalous behavior and repeat activity

Here are some examples of onboarding questions added to an existing loyalty account creation or incentive offer response:

- *Are you a current or previous member of our loyalty program?*
- *Have you previously utilized this promotion?*
- *Is this your first time using this free trial offer?*
- *Have you been a paying or free user of this service in the past 12 months?*
- *Did you send this exclusive offer to yourself from a different account?*

CONCLUSION

COVID-19 caused a cascade of behavioral and economic changes with a range of issues impacting businesses of all types. These changes shook the underlying assumptions and foundation of risk models while traditional and alternative credit reporting methods struggled to keep pace with the rapid rate of unemployment and new level of outstanding consumer debt.

Organizations changed how they could reach consumers quickly but struggled to handle the changing risks without either exposing themselves to fraud and credit risks or turning down a lot of potential business.

While these changes impacted industries across the board, there are themes and similarities that provide help to reduce the risks and better manage digital consumers and applicants. This primarily focused on cultivating new signals that are not contingent on past data or indications, because so much changed so fast. Organizations who could leverage behavioral components and signals found themselves in a much better position to navigate the risk landscape which was turned upside down almost overnight. There is no solution today that provides more actionable insight into digital friction and fraud, especially when you consider the need to keep up with a rapid pace of change in the post-pandemic environment.

Thinking about the examples of targeted onboarding and application questions, this is something any organization could add to their onboarding flow. The critical factor, however, is detecting anomalous behavior in response to these questions, which provides the ability to gain stronger insights around a consumer's intent and how much trust or confidence is instilled with each answer. While this is important and has always provided value, this is even more critical today as the value of several other methods for recognizing fraud and credit risks have begun to diminish.

ORGANIZATIONS WHO COULD LEVERAGE BEHAVIORAL COMPONENTS AND SIGNALS FOUND THEMSELVES IN A MUCH BETTER POSITION TO NAVIGATE THE RISK LANDSCAPE WHICH WAS TURNED UPSIDE DOWN ALMOST OVERNIGHT.

SEPARATING GENUINE FROM FRAUDULENT

Third Party Fraud - *"Are you...you?"*

Observing specific behavioral attributes contributing to Neuro-ID's third party fraud model, **we see a contextual narrative illuminating two actionable groups, and an opportunity to take action** with confidence based on the presence of potential fraud, or lack there of. The behavioral layer focuses on identity-related fields, where responses would typically come easily and draw from long-terms memory. When an applicant (or bot) clearly stumbles in what should be a simple task, it means something.

Minimum Hesitation for **'Personal Info'** Fields

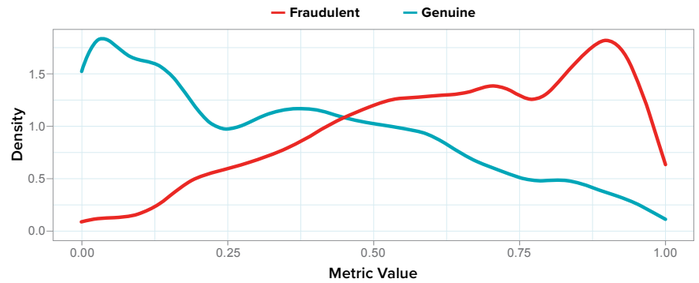


Fig 3.0 - Fraudulent applicants hesitate much longer than genuine applicants, who enter familiar information using long-term memory to respond. The distinction is pretty clear with each having the greatest density at the high or low points, respectively.

Maximum Interaction Time for **'Personal Info'** Fields

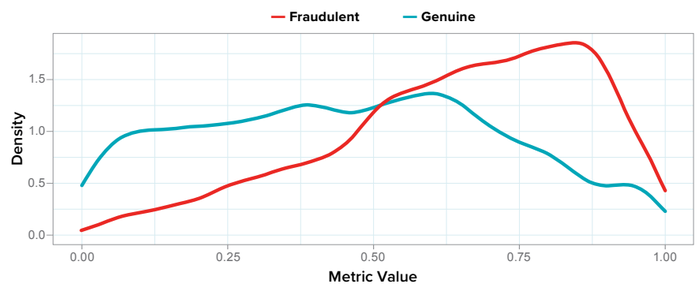


Fig 4.0 - Fraudulent applicants have a higher maximum interaction time entering personal information than genuine applicants. Again, genuine applicants responded more fluently, drawing on familiar information and long-term memory, reflected in a closer-to-normal distribution with some skew to the low side.

Figures 3.0, 4.0 - Applicant segmentation: the fraudulent group was comprised of the lowest scoring 10% and the genuine group from the highest scoring 10% for Neuro-ID's third party fraud model, correllated and tuned against comfirmed cases of third party fraud. The data for the model was taken from 5 different consumer lending forms between March 25, 2019 and August 2, 2020. Total sessions: 117,340. Number of Positive Outcomes (Not-fraud): 115,249. Number of Negative Outcomes (Fraud): 2,091. All of the attributes that went into the model are our quantiled attributes, which are on a scale of 0 to 1.

First Party Fraud - *"Is your information accurate?"*

Neuro-ID's first party fraud model provides a unique behavioral lens into the 'quality' of self-reported data. The real-time signal focused on fields relating to income and employment, measuring the speed and fluency of the applicant's response. **Again, the resulting data isolates applicants into two groups – fraudulent and genuine**. This is a key example of deriving predictive power from 'how' an answer is provided, and not the answer itself.

Minimum Interaction Time for **'Income'** Fields

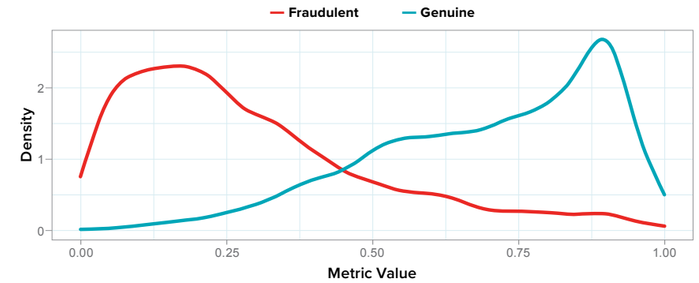


Fig 5.0 - The plot shows the minimum interaction time on all income fields that were interacted with in a session. Those who are genuine are more likely to have a higher minimum interaction time on income fields than those who are fraudulent. Genuine applicants historically respond in a deliberate manner to fully understand the question and respond in a proper, accurate fashion.

Minimum Typing Fluency for **'Income'** Fields

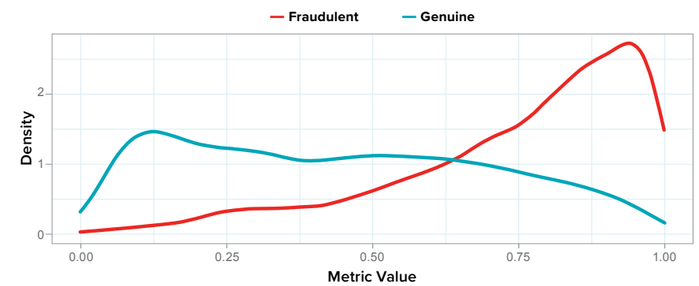


Fig 6.0 - The plot shows the minimum typing fluency on all income fields. Fraudulent applicants generally have a higher typing fluency on income fields than genuine applicants. This makes sense in the context of 1st party fraud since genuine applicants tend to be confused by the wording of the income fields and are unsure about what to enter.

Figures 5.0, 6.0 - Applicant segmentation: the fraudulent group was comprised of the lowest scoring 10% and the genuine group from the highest scoring 10% for Neuro-ID's first party fraud model, correllated and tuned against comfirmed cases of first party fraud. The data for the model was taken from 5 different consumer lending forms between December 31, 2018 and August 2, 2020. Total sessions: 89,104. Number of Positive Outcomes (Not-fraud): 83,623. Number of Negative Outcomes (Fraud): 5,481. All of the attributes that went into the model are our quantiled attributes, which are on a scale of 0 to 1.