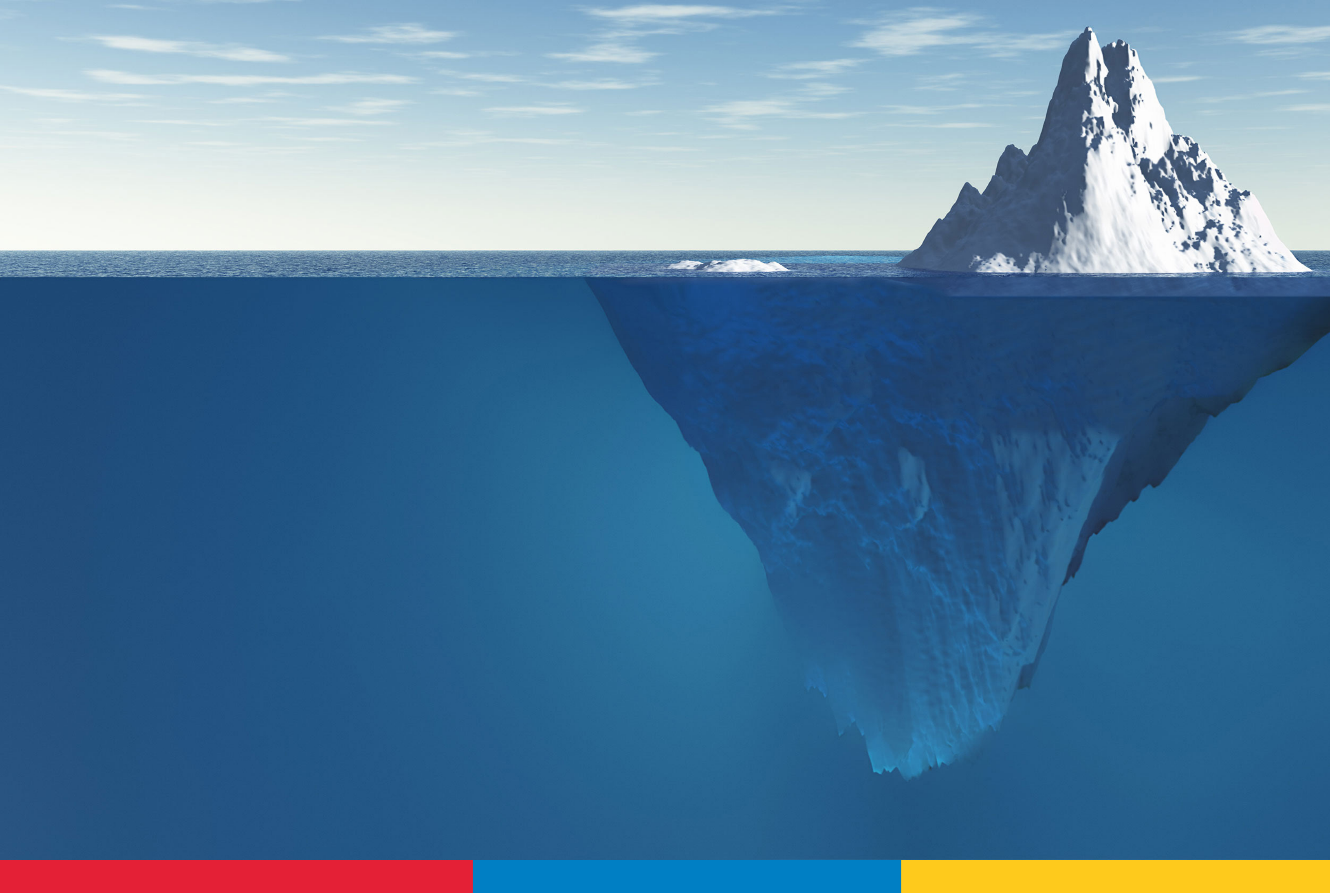


IF FRAUD IS NORMAL, WHY THE HELL ARE WE STILL LOSING SO MUCH REVENUE?

APRIL 2020

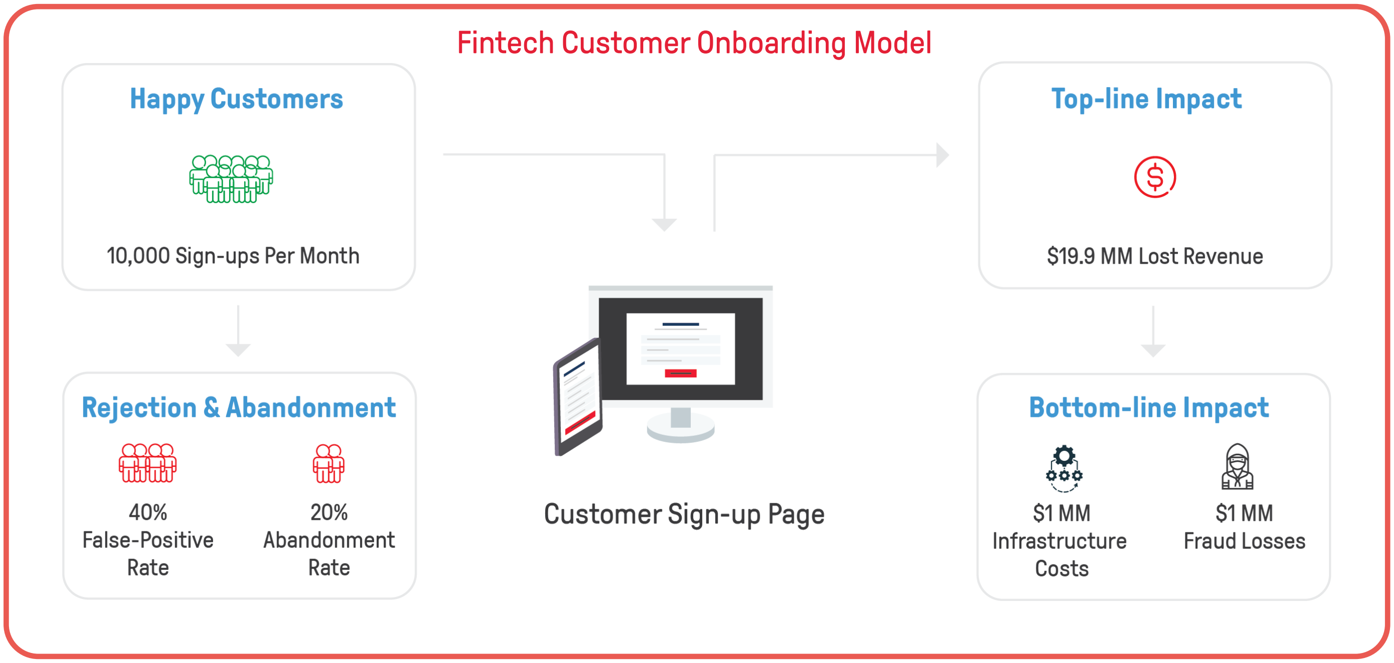
www.instnt.org | sales@instnt.org

YOU WANT MORE REVENUE AND ZERO FRAUD LOSSES.

Is it possible the focus on fraud is outweighing our ability to sign up more customers? Online businesses put delivering frictionless customer experience as a top priority, yet existing fraud prevention programs are blocking up to 40% of good customers. Then why do companies primarily focus on fraud versus improving their top-line growth?[1]

At Instnt, we think it's time to think differently about customer on-boarding. Top-Line growth and your bottom-line depend on it!

The customer onboarding model below reflects a fintech challenger bank that is signing up 10,000 happy customers a month. They are losing 4,000 customers due to a 40% false-positive rate and 2,000 customers due to poor sign-up form performance and customers abandoning the application process. Each customer is worth $300 annually. This bank is losing over $19 million in potential revenue annually! The IT team orchestrated their own customer onboarding stack and are struggling to scale the $1 million in technology and operating costs. Trying to keep the bad guys out and managing the manual reviews of the customers that make it through the online sign-up gauntlet is a challenge. Even then they are still losing over $1 million in fraud.



What if it were possible to cut the false-positive and abandonment rates in half? This smaller company would get a 30% revenue lift for the year and the bigger the financial institution the more potential.

Executives need to ask if the focus on fraud is outweighing their ability to sign-up more customers?

We believe the current balance between risk management and customer experience is all wrong. The pendulum has moved too far in the wrong direction where fraud reduction is the main focus and driver. This type of risk management is adversely impacting customer sign-ups, their perception of your brand and your revenue growth.

[1] Why 40% of consumers abandon banking applications; © Signicat 2018

At Instnt, we disagree with this approach, and although fraud is part of signing-up new customers, it shouldn't be costing you 30% of your potential revenue to fight it. The scale and unpredictability of fraud simply make it impossible for any company or business unit to win the battle alone. The risk and fear of fraud losses also force companies to implement draconian risk management controls that create dreadful customer experiences that are riddled with unnecessary friction.

Without exception, companies we speak with acknowledge customer onboarding is limiting their top-line growth and has an adverse effect on their bottom-line. Then why do they persist in orchestrating their own "whack-a-mole" solutions that deliver at best incremental results? We believe it's time to consider a different approach, one that includes collective intelligence and network effects powered by a new business model that can reduce the massive waste and poor performance of legacy solutions.

There is no silver bullet but there are three overarching industry practices and bottlenecks central to the current models being employed to stop new account fraud and account take over:

1. Dependence On Static Data From Major Credit Bureaus

Credit bureaus and other data providers are essentially monetizing hacked and stolen consumer data and repackaging user demographics. Moreover, the demographic of Millennials and GenZ that will be driving the economy for the next 50 years are all considered 'thin-file' by the credit bureaus. This falsely suggests that there isn't sufficient information about them in the on-demand economy they have spurred. Gartner, amongst others, has made it abudently clear that the reliance on shared secret data is an outdated approach. Yet it is endemic, over 90% of companies that facilitate digital account opening actually rely on shared secret models[2].

2. Point Solution Orchestration

Point solution orchestration involves the integration of third-party information and tools to de-risk potential customers. The goal is to assert a scored level of validation that the person on the other end of the transaction is a good customer, a real person engaged in signing-up for a product or service. Companies tend to orchestrate around waterfall risk models, applying the cheapest and simplest tools at the top of the stack. The further down the funnel they get, the more expensive and complex the solutions become. Built on the flawed assumption that access to more information and more tools will provide the ability to reduce the risks of various types of fraud.

Companies attempt to verify against many forms of identity information sources, capturing behavioral analysis, IP verification, device tagging, fraud checks, document verification, AML, and watchlist screening configured by human-defined rules. Companies orchestrate with solutions like Alloy and IDology or build their own home-grown orchestration engines, adding layers upon suites of different tools to create new account fraud detection stacks. The challenge they face is the technology waterfalls produce significant false positives. They continue to lose good customers as a consequence of the friction caused by the low performance of these waterfalls. Moreover, human defined orchestration rules need constant upkeep in a reactive rather than proactive manner, compared to modern machine learning approaches.

[2] Gartner Security and Risk Management Scenario Planning, 2020

Inevitably the engine doesn't scale. Companies limit how many new customers they accept and employ large teams of people to catch and manually review the customers that fall out of the digital process. The vicious cycle of fraud growth and the desire for better business results supports a cottage industry of hundreds of vendors. This is ultimately vendor roulette and literally a gamble whereby companies have hundreds of options to choose from, making it harder for companies to know what to use and how to align the different options. IT, Risk and Compliance are treated as cost centers and naturally always fighting for budget. Underfunded teams struggle to source the expertise to get it right more than 95% of the time, making it mathematically and financially unviable to balance growth and fraud loss expectations.

3. Business Model Conflict

The third problem we face is more serious and intractable. Business model conflict occurs when your company takes all of the liability and risk for the services procured during the orchestration process. Independent orchestration locks companies into transactional pricing while at the same time removing any potential for liability assurance due to the custom nature of the implementation. Vendors explicitly callout the lack of liability indemnification because your team is responsible for tuning risk controls and fraud loss decision-making.

The continued use of personal identifiable information by credit bureaus and other static data providers also creates its own business model conflict. These vendors are essentially monetizing consumer data sources that have already been hacked multiple times. Using the same user demographic information to support the technology orchestration model explained earlier. These are the very breeding grounds for synthetic ID fraud in the first place. This is where the bad guys go to create the fraudulent identities we are all trying to protect against.

Shouldn't your company be paying for performance, paying for the value received from good customers enabled and the fraud losses eliminated? Rather than playing vendor roulette and hoping your team has the ability to craft a better mousetrap!

You have two choices. You can either build your own stack and take all of the losses, deployment complexity, and limit your performance. Or you can use a managed service and remove the fraud from your bottom-line and rapidly improve your top-line! At Instnt, we are building a coalition-based approach to customer onboarding, with a more environmentally friendly business model that generates network effects and generative sources of value for our customers.

JOIN THE INSTNT COMMUNITY TODAY.

We have formed a discussion group to deal with the Orchestration, Business Model and Fraud challenges we have discussed here. If you want to have an impact and believe your company might benefit from the insights, join the discussion here.

#singlesignup