WHITE PAPER

Socure Unit21

KYC as a Driver for Customer Acquisition, Brand Confidence, and Incremental Revenue

In 2017, 80% of new customers walked into a brick-and-mortar bank to open their account. Just three years later that number dropped to 37%, with the majority of customers using digital banking to open accounts and manage their money. Online fraud targeted at those digital banking customers accelerated at an even faster rate, rising by more than 52% in just the one year between 2019 and 2020.[1]

When reading statistics like those, compliance, AML, and anti-fraud professionals often first think of how to better protect their institutions in our brave new digital economy. But when every technological evolution opens new entry points for stealing identities, attacking financial systems, and laundering funds, it's just as important for your customers to trust *you* as it is for you to trust *them*.

That trust isn't built from just one interaction, but rather from a continuous Know Your Customer (KYC) and Customer Identification Program (CIP) process that builds a strong foundation of reliable identification and protection. True KYC is much more than a single score or output—it's a dynamic, ongoing process that starts at onboarding and continues throughout the business-customer relationship. In our world of increasing digital vulnerabilities, that relationship is more important than ever. By making sure that you have onboarded the most trustworthy customers into your banking ecosystem, you're protecting yourself and also creating a competitive differentiator level for your customers who know it's not a matter of if their identity will be stolen, it's only a question of when, and through what means.

[1] *Identity Theft and Credit Card Fraud Statistics for 2021*, Motley Fool, 2021

> “The ability to execute trusted, secure transactions is a core mandate for legacy financial institutions looking to maintain market share as the landscape of alternative digital and mobile financial service options continues to expand. Connected customers, fatigued by . . . unprecedented personal data breaches and able to select from a growing array of innovative financial products, make their choices based on trust . . . this means that trust is a core product offering—as quantifiable and impactful as any credit vehicle. ”
>
> – *Digital Identity: The Foundation for Trusted Transactions in Financial Services, The Capco Institute Journal of Financial Transformation*

KYC and the Challenge of Trust

At its core, KYC represents the risk of your customer to your organization. It is intended to help you prioritize the review and treatment of application and transactional risk. For example: a customer opens a checking account where they deposit their paycheck and then spend that money on their day-to-day expenses. Without other major risk factors, a typical KYC evaluation would bucket this person as a low-risk customer. But if a low-risk customer suddenly deposits a large amount of money and takes it out in cash, a transactional alert would go off. The disposition and prioritization of such an alert would fall below an identical customer who had landed in a high risk category at initial onboarding assessment, when they go through a CIP gate (the first step in KYC).

That initial onboarding risk assessment is key, both for you and for your customer. As the first step to “knowing” your customer, CIP is the first time you and a prospective customer “meet.” It’s the first chance you have to evaluate them, and vice-versa. From the compliance side, by forming a risk-assessed reasonable belief that you know the true identity of the customer, you can in part reduce the likelihood of fraudulent actors and of identity theft. But on the customer side, CIP can contribute to friction and create a poor customer relationship from this first “meeting.” Like with any first impression, a positive CIP experience at onboarding can go a long way to cement the relationship, while a negative experience can cause one or both parties to walk away from the relationship. How you handle your CIP process, how you choose your CIP solutions, and how you deploy those solutions within the greater KYC risk assessment process all play a part in onboarding success.

Beyond Onboarding: KYC is Not One-Size-Fits-All

While “knowing” your customer is a universal component of building trust on both ends, the actual KYC risk scoring process does not have a simple, one-size-fits-all approach. Quite the opposite, your KYC process must contain robust customer due diligence (CDD) and enhanced due diligence (EDD) procedures, reflective of your specific organizational risks and goals. Failure to confirm your customers’ identities with due diligence requirements can result in audits, heavy fines, reputational damage, or worse—so of course you care about accurate KYC risk scores. But if you’re like many of your compliance professional peers, caring about KYC processes does not mean you’ve found the best ways to optimize your system against today’s evolving digital threats.

KYC risk scoring is based on the idea that the first step towards strong fraud prevention is knowing your customer and their risks. The stakes are high: since 2008, U.S. banks have paid more $30 billion in regulatory penalties due to “corruption, AML-related, and MiFID compliance breaches” related to financial crime.[2] The reputational impact and cost isn’t as easy to calculate in raw numbers, but is often even more damaging.

KYC plays a critical role in enabling financial companies to perform initial risk assessments by identifying and declining those customers who may bring high risk, while accepting those who bring low risk. The CIP step of KYC guarantees that new customers can be clearly identified and verified from day one. This CIP stage creates a foundation for reliable compliance, even with shifting regulatory regimes, so you establish a secure customer relationship right at onboarding for a continued defense against fraud across the business-customer lifetime.

[2] *https://financialinstitutionsfines.com/*

> "While recent cases have shown that the on-boarding of high-risk and unlawful clients can lead to increasingly punitive fines and severe reputational damage, legitimate clients also incur disturbing "privacy taxes." This breach of client trust only compounds operational and reputational harm, causing some customers to close their accounts with the delinquent institution and seek new banking partners."
>
> *– How banks can turn the KYC compliance challenge into a competitive advantage, Thomson Reuters*

CIP/KYC for Customer Confidence on Both Sides

Like any foundation, CIP/KYC must be solid, trustworthy, and reliable. Any holes or weaknesses, and the whole structure will collapse. However, legacy identity verification technologies create a foundation built on an extremely limited set of identity data by utilizing only the regulatory requirements for data collection. These legacy evaluations of identity and trustworthiness typically rely solely on a decades-old credit scoring model to determine whether an individual is trustworthy enough to enter into a transaction. This type of verification is a blunt and shallow approach that excludes millions of thin-credit and hard-to-identify populations, especially Gen Z, millennial, and new-to-country consumers who may not have the credit history or identity documents to be trusted by traditional CIP/KYC.

CIP/KYC with poor data matching inevitably creates foundational cracks for bad actors to slip through. As every compliance officer knows, fraudsters and money launderers evolve as quickly as the technological tools to contain them. More than 15.4 million Americans were the victims of identity fraud in 2016, with losses totaling $16 billion. Worldwide identity theft costs are estimated to be at least $221 billion. An estimated 1 in 9 digital account creation attempts are fraudulent, as are around 1 in 20 digital login attempts.[3] In addition, from an AML perspective, synthetic identities pose a real, tangible risk to the organization. Many threat networks create fleets of fictitious borrowers. Some synthetic identities schemes have been utilized to commit fraud or integrate and layer funds in money laundering.

The customers you let in the door and how you manage your onboarding risk and identify verification to establish trust right from the start are key elements in the process of fraud prevention and customer retention. Because so many consumers have been victimized by identity fraud, KYC has become a core competitive offering for financial institutions: as quantifiable and impactful as any other revenue influencer. The best compliance teams will treat it as such.

Accelerate Growth and Enhance Customer Experience with Unit 21

In partnership with Socure, Unit21's Identity Verification solution empowers risk and compliance teams to automate decisions using a customizable modeling engine to approve more customers and increase revenue. Unit21 features custom workflows to cater to your specific use cases, synthetic identity checks to ensure that entities submitting falsified personal identifiable information can be easily identified, and link analysis - a visual representation of your data that will enable you to take a step back and view the whole picture, drawing links between entities and events that would otherwise be impossible to unveil. Our solution also tracks and stores every action taken on our dashboard as an auditable trail, allowing our customers like Chime, Intuit, and Coinbase to defend against fraud with better data. Discover how Unit21's Identity Verification Software can help you accelerate customer growth today.

Contact a Unit21 Identity Verification expert to learn more.

Socure Unit21

[3] *Identity Fraud: Securing the Connected Life, Javelin Identity Fraud Report*