494 words

Protecting Users, Reducing Fraud, and Complying with KYC Through Identity Verification

In the last 90 days, events in the news have underscored the need for digital identity verification.

In 2015, regulators ordered Wells Fargo wholesale division executives to repair their non-compliant, anti-money laundering (AML) policies. The San Francisco-based bank says three years isn't enough time to overhaul their risk and compliance behavior. Therefore, they asked to extend the June 30 deadline.

If the Office of the Comptroller of the Currency (OCC) denies the extension, Wells Fargo may add another fine to their $12 billion plus since 2000 and 20 penalty records since 2015. Is there a connection between a bank's alarming non-compliance statistics and rising awareness of social media fraud? Do social media platforms need to prioritize customer identity programs? Yes, and yes, because regulators are watching closely.

While Wells struggles to achieve AML compliance, social media companies face other challenges. With fictitious Facebook ads, unverified Tweets creating fake news, and pretend influencers driving consumer behavior on Instagram, customer identification programs are critical. They protect users, reduce fraud, and comply with KYC regulations.

A 2017 study by University of Southern California and Indiana University discovered up to 15 percent of Twitter accounts were actually bots rather than real people. Although this study occurred a full year before Twitter clamped down on sham accounts, 2018 research revealed about 10 percent of Twitter accounts are still spammers or bots. Identify verification could help block phony social media accounts, reduce fake news, and mitigate the underlying threats posed by unverified users.

According to Scientific American's Peter Bruce, the fact Cambridge Analytica violated user privacy by harvesting and sharing personal Facebook data is less of a concern than how easily "con men, political demagogues, and thieves" twist social media platforms toward arguably dangerous ends. Bruce wonders if "deploying new [Artificial Intelligence] tools that can proactively catch fake accounts" will protect our privacy and identities. What makes these social networks so susceptible to corruption?

Some say it's simply the nature of the Internet and mobile beasts. Al Pascual, Javelin's SVP Research and Head of Fraud Security explains, "Digital channels have exposed the vulnerabilities inherent in the traditional identity verification process, which for many institutions was designed to meet regulatory requirements – not vet applicants for fraud. These vulnerabilities contribute to record rates of identity fraud. "

Facebook co-founder and CEO Mark Zuckerberg recently told Congress, "We're going to verify the identity of any advertiser who's running a political or issue-related ad." According to the NY Times, Facebook will work to prevent identify fraud among advertisers by authenticating government-issued ID belonging to the person buying the ads. Time will tell if Facebook's customer identity verification system works.

[Company/Name/Title] only needs 25 words to drive home the core message: **"Companies that make identity verification the cornerstone for how they operate and engage with their customers are the ones that will thrive, not just survive."**

Do you want your organization to thrive or simply survive? Protect your customers and ensure AML compliance with [Company].