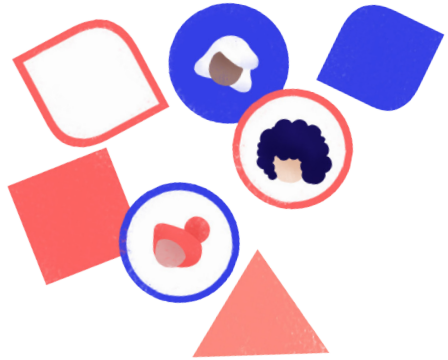
Financial Services, Fraud and the Future of Digital Onboarding

onfido

Contents

The changing face of identity



The identity industry is changing. Many of the identity indicators we took for granted are no longer fit for purpose. Social Security Numbers (SSNs) were never meant to be a national identifier, of course. But for decades, they have been the key proof of identity for millions of Americans. We expected the SSN to solve a problem that it was never designed for. And with the additional challenge of widespread digital onboarding, it can no longer carry that burden.

Cellphone ownership is another identifier that seemed promising. But, like SSNs, SIM cards and handsets were not designed for that purpose. And, like SSNs, their flaws have now rendered the system ineffective—and even dangerous—for use in digital onboarding.

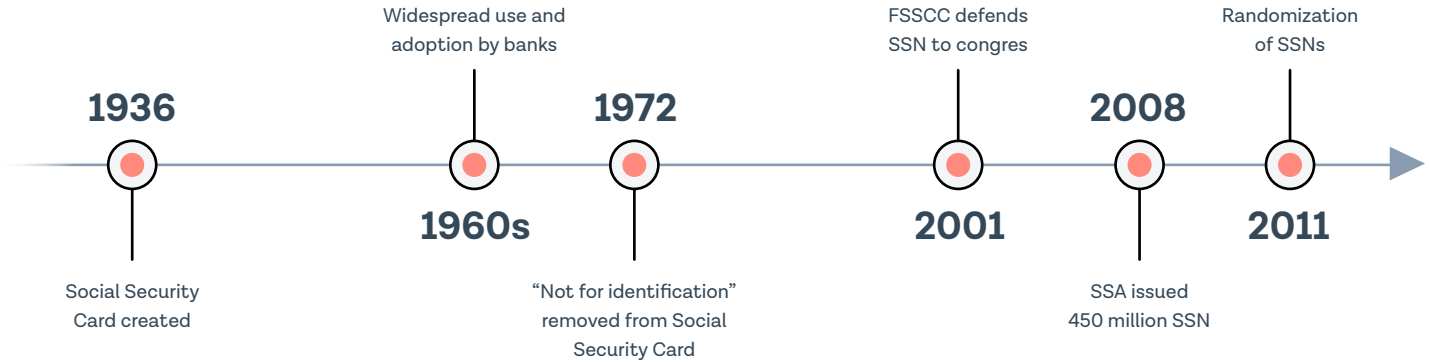
And it's not just the identifiers we use that are changing. Regulation is also changing the face of identity verification. New Customer Due Diligence (CDD) and Know Your Customer (KYC) regulation is raising new challenges for smooth and secure user onboarding, and that trend looks set to continue.

If we have learned anything from the SSN, it is that any future identity solution needs to be designed specifically for that purpose. New solutions will need new thinking, and new technology.

Identity is changing faster than ever. And the future belongs to those who can keep up.

Why numerical identifiers are no longer fit for purpose

At their inception in 1936, Social Security Numbers (SSNs) were a way of identifying how long people had worked, and therefore how much of a pension they were owed. Over the years, they increasingly started being used as unique identifiers— but that's never what they were supposed to be. Changes in regulation reshaped the SSN over its lifetime:



1936: Social Security card created to track the earnings histories of US workers, for determining Social Security benefit entitlement and computing benefit levels. They were not meant to be a national identifier.

1960s: Use was widespread. Banks used it to match accounts of "millions of Joneses, Williamses, Johnsons" and when banks adopted it, that legitimized it.

1972: "Not for identification" removed from card.

2001: Financial Services Sector Coordinating Council told congress that by using SSN to verify individual identities, credit reporting firms can quickly provide financial institutions with accurate credit histories.

Using SSNs for identity verification is now a process riddled with vulnerabilities.

And what's more, the Social Security Association (SSA), doesn't actually have the authority to stop anyone from using an SSN that's not legally theirs.

As we've moved away from SSNs, we've replaced them with another unique numerical identifier—our cell phone numbers. But they're not secure either, as victims of the 2018 T-Mobile porting scam have learned. One such victim lost $3,500 in one month, had $6,000 transferred from her account—and had to wait 21 days for her bank to return the funds. How did this happen? Scammers took advantage of the loophole in this kind of 2-factor authentication, which sends verification codes to a user's cell phone as a form of identity assurance.

If scammers can take over that user's cell number, porting it to another provider, they get access to a treasure trove of that user's services, from banking to social media. Because, once a phone is ported, all of the other data connected to that phone number is compromised.

3 key changes in regulation

1 NIST 800-63A Section 5.1.3.2

NIST regulations have recommended that we move away from using cell phones in 2-factor authentication, for security reasons.

Digital Identity Guidelines Enrollment and Identity Proofing
'Due to the risk that SMS messages may be intercepted or redirected, implementers of new systems should carefully consider alternative authenticators.'

2 The Banking Reform Act

S2155 Economic Growth, Regulatory Relief and Consumer Protection Act Making online banking initiation legal and easy: Scanned ID doc images have to be deleted after account opening. It's not yet specified how quickly this needs to be done, but businesses won't be able to keep that information.

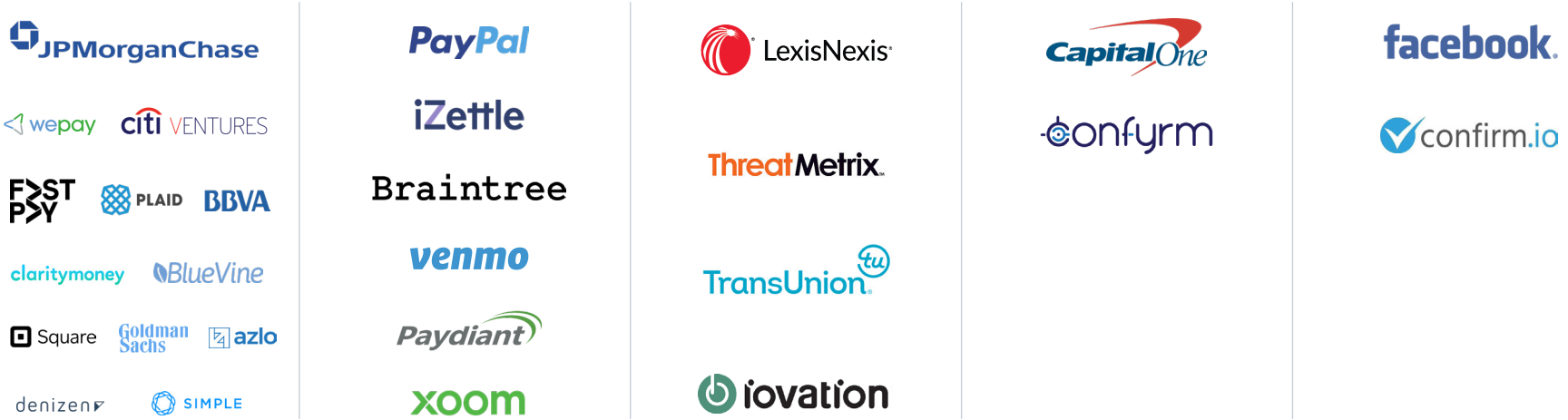
Reducing Identity Fraud: You are now required to go direct to the source to confirm a person's

3 GDPR

In Europe, the EU's new General Data Protection Regulation (or GDPR), which went into effect as of May 25, 2018, sets out a new and rigorous set of data privacy requirements. Under GDPR, companies have to implement data protection systems, including policies and procedures for managing and protecting data.

You can also see this trend in the USA. California's Consumer Privacy Act will be live in January 2019. Congress passed the MOBILE Act in 2017. Overall, in most countries, regulation is moving toward more privacy protection for consumers.

Identity today



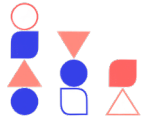
Current solutions are using a combination of social media profiles, passwords, KBAs, Social Security Numbers, IP address locations, behavioral analytics and device profiling to authenticate identities.

Things like these build up a cyber identity footprint. If you authenticate them, you can prove that this footprint exists. But not who has made it. That's because these things only prove an identity—they don't trace it back to a real, living human. Linking a cyber identity to a physical, human identity is hard to do. But it's essential to building a level of trust and security online. And the best solutions will find a way to do this without adding friction to any digital onboarding experience.

Best practice

Use biometrics

According to IBM, 87% of all adults will be comfortable with using biometrics in the future. Adding a biometric step to your identity verification process—either at onboarding, for ongoing authentication or at service upgrade stage—can tie a real and live person to a verified government ID. This gives you the only true assurance that the person accessing your platform is the authentic owner of the identity they have claimed. What's more, biometrics stop these fraud attempts from being truly scalable. Fraudsters want to find a way of committing fraud, and to repeat it again and again. Biometrics make it harder for that to happen.



Tailor to your needs

A financial services provider might need more robust vetting within their onboarding process than a Trust Marketplace business. Take a risk-based approach, so you can balance appropriate levels of security and friction. Not every user will need to go through heavy vetting. It may only be needed when they reach a certain threshold—like higher value transactions, or more premium levels of service.

Think beyond SSN

For an identity system to work, it needs not only to be trusted, but convenient. Otherwise user behavior will preclude its use. The ability to port, or transfer, identity between providers safely and securely will be key to this. It removes friction for consumers, and reduces cost for businesses.

New ways of thinking about identity management, including decentralized and self-sovereign models, bridge offline identities (government issued identity documents) with digital credentials created upon verification of an identity claim. Get involved with initiatives like the Better Identity Coalition to help shape regulatory frameworks and keep your business ahead of the curve.

Get in touch:
info@onfido.com
https://onfido.com

San Francisco | New York | **London** | Lisbon | **New Delhi** | Singapore