Fintech Takes

The Digital Identity Paradigm Shift

2024

PLAID

Written by
Alex Johnson

Let's start with some statistics:

- According to the **Identity Theft Resource Center**, there were 3,205 data compromises in 2023, a 78% increase from 2022 and a new record, topping the previous all-time high of 1,860 set in 2021.
- Total P2P payment fraud losses in the U.S. reached an estimated $1.7 billion in 2022, a 90% increase over 2021, according to **Deloitte**. Complaints to the Consumer Financial Protection Bureau (CFPB) regarding payment apps increased 164% between 2019 and 2021.
- Based on an analysis of the CFPB's **consumer complaints database**, the number of complaints regarding the credit reporting industry increased by more than 650% between 2019 and 2023. During that same time period, all other complaint categories - debt collection, credit card, mortgage, checking & saving - stayed flat or only increased modestly.
- In 2023, U.S. lenders' exposure to synthetic identity fraud - in which fraudsters utilize stolen pieces of personally identifiable information (PII) to create new fictitious identities at the credit bureaus - was nearly $3 billion, a 20% increase from 2022, according to **TransUnion**.
- FinCen recently **found** that 42% of Bank Secrecy Act (BSA) reports filed in 2021 were related to identity fraud, meaning that an estimated $212 billion in suspicious activity that year was the direct result of failures in banks' identity verification processes.

If all of this strikes you as A.) bad, and B.) trending in the wrong direction, I agree with you.

And the question that we, as an industry, need to ask is, "Why is this happening? Why is it that, at a time when we've never had more data and analytics and technology to throw at identity verification and fraud prevention, things feel like they're getting worse?"

My answer is that it feels this way because we are in the early stages of a paradigm shift.

Out With the Old

In science, a paradigm is a set of baseline assumptions about physics, biology, and other scientific disciplines that experts take for granted as true. Scientists measure their experiments and observations in relation to these assumptions, with an expectation that none of their discoveries will fundamentally challenge them.

A paradigm shift happens when scientists start observing new phenomena that don't conform to the accepted assumptions. The first couple of times this happens, scientists will often dismiss the unexpected results as flukes or mistakes (all humans, even scientists, have a natural dislike of having their worldviews challenged). Eventually, though, enough evidence that doesn't fit the prevailing paradigm accumulates, and scientists develop a new set of assumptions – a new paradigm – to reconcile the inconsistencies and to help them better predict the results of their future experiments. The transition from a geocentric cosmological model to a heliocentric model, the shift from Newtonian physics to general relativity, and the jump from classical mechanics to quantum mechanics are all examples of major scientific paradigm shifts.

Most of us working in financial services aren't scientists, but I do think that we've all been operating under a set of assumptions for how we can safely facilitate financial transactions in a digital-centric world, and those assumptions are, as we just covered, being increasingly challenged.

Perhaps it's time for a paradigm shift.

Branches and Bad Reputations

Banks are required to know their customers. This requirement exists (in its many different regulatory forms) in order to protect banks and their customers from fraud and to enable banks to help the government identify and hopefully prevent money laundering.

Until very recently, banks' Know Your Customer (KYC) processes were fairly straightforward. Banking was an activity that was conducted, for the most part, in person. In branches. The bank knew its customers because the people working in the bank branch literally knew them, personally.

Sure, the bank would take certain extra precautions, like requiring a government-issued ID to open an account and keeping a signature card on file at the branch to verify customers' checks. But mainly, KYC worked because banking was a relationship business.

Credit was very different.

As Josh Lauer explains in his excellent book "**Creditworthy: A History of Consumer Surveillance and Financial Identity in America**," up until the 1950s, banks in the U.S. did very little unsecured consumer lending. Instead, this lending was almost exclusively the province of merchants.

The challenge was figuring out which customers to offer credit to. This was much trickier than KYC. It's one thing to know who Alex Johnson is; it's another to feel confident that he is a responsible credit user at all the stores he shops at. The only way to attain that confidence was for merchants to share that information with each other.

Enter the credit bureaus.

In the late 1800s and early 1900s, credit bureaus were local organizations (often nonprofits) formed by merchants in specific cities.

By the 1950s, credit bureaus had grown larger and more organized (and more focused on profit). They increasingly leveraged computer databases to improve the efficiency (and, thus, the scale) of their operations, which just so happened to be around the same time that banks were becoming more involved in unsecured consumer lending (giving the bureaus a whole new market to sell to).

By the late 1960s, the growing reach and technological sophistication of the credit reporting industry caused a bit of a panic in Congress, leading to extensive congressional hearings and, eventually, the passage of the Fair Credit Reporting Act (FCRA) – one of the first data privacy laws of the information age – in 1970.

Despite the burdens of the FCRA, the credit bureau industry continued to rapidly digitize, and by 1973, all of the credit bureaus in major metropolitan areas were fully digitized, and by the mid-1980s, the industry had consolidated down to just a handful of large national credit bureaus.

All the while, the industry continued to project confidence in its ability to safeguard Americans' personal data, just as John L. Spafford, (President of the Associated Credit Bureaus of America) told Congress they would in 1968:

- We have protected privacy for the past 60 years, and we believe we can protect it in the future. We believe we can do it with computers – and frankly, gentlemen, we believe we can do it with whatever comes after computers.

("With whatever comes after computers." File that part of the quote away. We'll return to it later.)

Digital Identity: Take One (Stretching The Bureaus As Far As We Can)

So, this is where we were, as an industry, in the early 2000s - KYC was (mostly) analog, credit risk evaluation was (mostly) digital, and everyone in the industry was (mostly) satisfied.

Then came the internet!

Suddenly consumers were applying for products and interacting with their financial services providers predominantly (or entirely) online.

Banks' credit risk evaluation processes adapted fairly well to this shift, but KYC was a problem. Requiring a consumer to complete the online account opening process by driving to the branch to provide proof of identity or to sign a signature card was a non-starter.

So the credit bureaus stepped in. While credit files weren't designed to function as digital IDs, the bureaus found that they, uniquely, had the data coverage and distribution to immediately help banks solve their digital KYC challenges. They developed a suite of identity solutions; some simple (packaging the basic identity data - name, address, SSN - into its own verification product, sometimes referred to as 'credit header data') and some more complex (knowledge-based authentication questions that leveraged the bureaus' data and that only legitimate consumers would know the answers to).

Two things are important to note here:

1. The credit bureaus' expansion into the identity verification space was opportunistic, enabled by their established relationships with banks and their ability to twist their core product into a new shape that could help solve the digital KYC problem. They didn't win this business by building the objectively best solution for digital identity.
2. That said, the credit bureaus do deliver (both in credit risk underwriting and identity verification) a very convenient experience for consumers. This is incredibly important to understand. For all their flaws, there is something magical (from a UX perspective) in being able to supply a few pieces of information (credit header data) and, with little additional work, unlock access to a vast array of financial products and experiences. The design and data coverage of the U.S. credit reporting system is what enables this.

This system worked reasonably well in the early days of digital banking, when banks were the dominant providers of financial products and services, and consumers' expectations for what they could accomplish financially using the Internet were modest.

Digital Identity: Take Two (Fintech Challenges & Innovations)

You know the next chapter of the story. B2C fintech companies appeared, offering compelling, digitally-native financial products and experiences. They succeeded wildly in raising consumers' expectations and unbundling their financial lives (according to Plaid's excellent annual report - **The Fintech Effect** - the average consumer reported last year that they use between three to four fintech apps and 20% projected that they would be using six or more digital apps within six months - an increase from 14% in 2020.)

And this brings us to where are today - a fractured, fast-moving, highly competitive financial services ecosystem where digital-only experiences, products, and business models are increasingly dominant.

The identity infrastructure underpinning this ecosystem is beginning to crack under the pressure.

The escalating cascade of data compromises has put an incredible amount of PII in the hands of bad actors, which they can use to defeat even the most sophisticated knowledge-based authentication processes and to cultivate new synthetic identities to seed inside the credit bureaus. Financial services providers - operating in today's intensely competitive market - are loath to impose additional friction on customers and prospects for fear of driving down their conversion rates. And new technologies - such as generative AI - are giving fraudsters terrifyingly powerful and cost-effective tools to up their game with (**this recent news story** about a finance worker being tricked by AI-generated deepfake videos of his colleagues into sending $25 million to fraudsters is every company's worst nightmare.)

Now, to be fair, fintech has done its best to help the industry overcome these growing identity verification and fraud management challenges. Today, we have a whole world of new point solutions, designed to address the gaps created by the digitization of financial services. These include ID scanning (which eliminates the need for in-person identity document presentment and verification), device and geolocation data (identifying the physical location and assessing the unique characteristics of the computer or mobile device that a consumer is using), behavioral biometrics (which help detect suspicious digital body language), and a host of new anti-fraud generative AI tools that clever technologists are building right now.

These incremental innovations have certainly helped relieve the pressure, but as evidenced by the growing rate of identity-based fraud, they are not sufficient to fully solve the problem.

It has gotten so precarious that consumers, particularly younger consumers, have actually raised their hands and asked their financial services providers to add a little friction to their digital products and experiences in order to make them safer. According to Plaid's Fintech Effect report:

- 76% of consumers said that they'd prefer to verify their identity to prove that they are who they say they are.
- 65% said they were willing to take a selfie and a picture of their driver's license to protect themselves from fraud when using a financial application.
- 64% said they feel safer using a digital financial product when they're required to provide identifying information, like a photo of their driver's license (for Millennials, that percentage is 76%).

Consumers are asking financial services providers to make them do more work in order to use their products!

If that's not evidence that we're on the precipice of a paradigm shift in digital identity, I don't know what is.

The question, though, is what might a new paradigm for digital identity look like?

Digital Identity: Take Three (A New Paradigm)

I'll start by saying that this is a question that folks much smarter than me have been obsessing over for a long time. In this section of the essay, I'll be building on their thoughts extensively. If you want to dive deeper into the weeds on these ideas, let me know, and I'll be happy to connect you with some expert resources. **This report** from the World Economic Forum is a great place to start.

Before we get into the nitty-gritty of how a more thoughtfully designed digital identity system could work, I want to acknowledge a couple of quick points:

1.) There is an obvious solution to the problem of digital identity in the U.S. - a centralized, government-run national identity system that allows for the creation, provisioning, and ongoing management of physical and digital identity credentials.

[He ducks as heavy objects are angrily hurled at his head.]

I know. I know, I know! We don't do that kinda thing here. Even though there are plenty of other countries that have successfully created electronic identification (eID) systems without anything bad happening, I know it'll never happen here. I just wanted to mention it!

It's also worth pointing out that the lack of a national identity infrastructure makes it that much more important for private market alternatives to prioritize portability - the ability to reuse identity credentials across multiple apps/products/ecosystems (Plaid's '**Verify Once, Verify Everywhere**' feature is a recent example of a good step in this direction).

2.) Despite an unwillingness to address this problem on a national level, some progress on this same general concept is being made, at a state level, although progress is slow and uneven.

Jason Mikula at Fintech Business Weekly **reported** a while ago that Apple was quietly in the process of signing deals with state DMVs in order to integrate verified driver's licenses from those states into Apple's Wallet app (with consumer permission). These contracts aren't particularly favorable to the states (shocking that DMV employees weren't able to out-negotiate a $2 trillion corporation). Currently, Apple is able to support digital driver's licenses from Arizona, Georgia, Colorado, and Maryland.

Apple's progress on this project has been glacially slow (and may have even regressed a bit?), likely complicated by other states' efforts to establish their own digital identity solutions. California, for instance, is in the midst of a **pilot program** for its new mobile driver's license (mDL), which currently requires users to download a separate app (no integrations with Apple's or Google's wallets) and can only be used in a small number of places.

3.) The foundation of our new paradigm for digital identity can't be based solely on something you know.

Of the three factors of authentication - something you know (password, answers to KBA questions, etc.), something you have (smartcard, hardware token, etc.), and something you are (fingerprint, facial recognition, etc.) - something you know is the most vulnerable, thanks to the constant data breaches that we all experience.

The good news, returning to that John Spafford quote - we believe we can protect privacy with computers and, frankly, with whatever comes after computers - is that we now know what the next thing after computers is.

Smartphones!

We now have the pieces that we need to build a new paradigm for digital identity!

How It Could Work

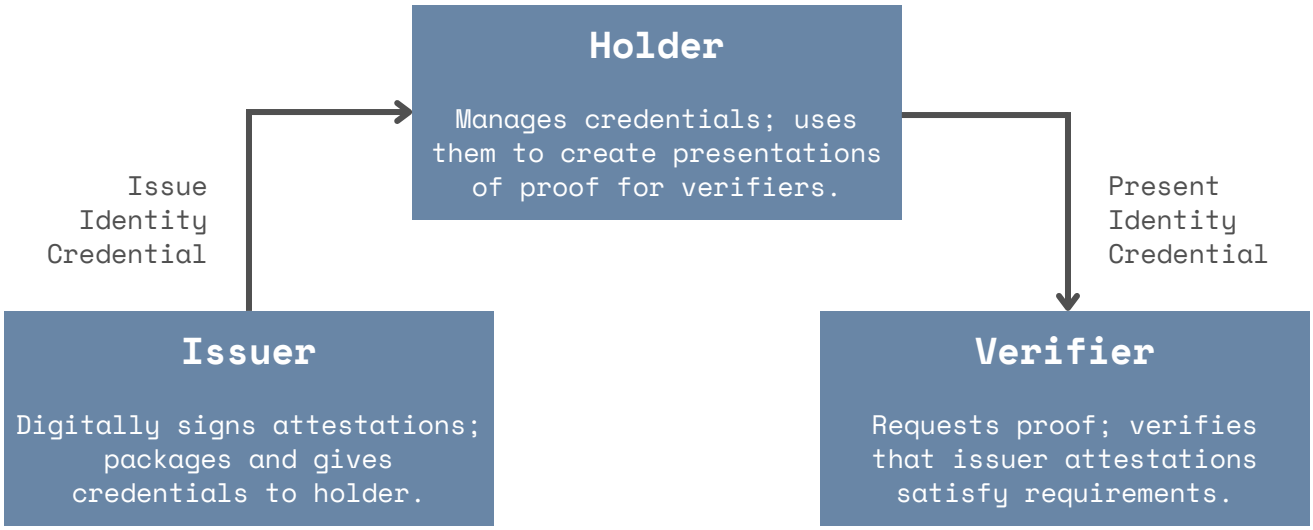
The general framework that I like for digital identity is decentralized ID.

> *(Editor's note - I know the term "decentralized" might give you traumatic flashbacks to 2021. Rest assured, my use of the term has nothing to do with the web3/crypto industry.)*

It's a three-party model:

1. Issuers - Government and non-government entities that can credibly attest to specific identity characteristics (a state DMV, for example, can credibly attest to a number of different characteristics, including name, age, and address) and issue credentials associated with those characteristics.
2. Holder - Individuals who are able to claim identity characteristics from issuers, manage the resulting credentials, and use them to prove claims about themselves.
3. Verifier - Government and non-government entities that require verification of identity characteristics in order to provide holders with products or services. Verifiers can request and verify proof of a specific identity characteristic or characteristics (e.g., a bouncer checking to see if you're 21 years or older).

Here's a diagram of what this model looks like:



One neat thing about this model is that, with the technology that we have today, it can be implemented in an extremely secure and privacy-preserving way.

The holder can claim and manage their identity credentials through a digital wallet app that is cryptographically secured on a smartphone and accessed through biometric verification (the smartphone satisfies both the 'something you have' and 'something you are' authentication factors).

And communication between the issuer, holder, and verifier can be facilitated through verifiable credentials (cryptographically secured digital credentials) and zero-knowledge proofs (a cryptographic technique that allows one party to convince another party that a certain statement is true without revealing the underlying data that proves the statement is true.)

The other neat thing about this model is that it creates a clearer delineation of roles within the digital identity ecosystem and a more level playing field for companies to compete within those roles.

Now, to be fair, some roles will likely be less competitive than others. For example, given the control they have over the hardware and operating system, Apple and Google clearly have pole position in the digital wallet race, over the likes of Paze, the California Department of Motor Vehicles, and random web3 wallets.

On the other hand, I expect that we'll see an intense level of competition within the issuer role, as any company with a large, trusted network of holders and verifiers will be tempted to try and become a credible attestor of identity.

Which company wins in this identity issuer role will depend on a few factors, in my humble opinion:

- **Breadth** – Network effects matter. The value of an identity credential is directly proportional to the number of potential verifiers that would trust it and to the number of holders for whom a credential could be issued. This is an area of strength for the credit bureaus, as well as other established network businesses that operate in heavily regulated industries (e.g. Plaid, Clear, ID.me).

- **Depth** – As we've discussed, there are levels to identity. The basic identity characteristics that can be used to satisfy KYC requirements are table stakes, but much of the value that can be provided by issuers will depend on their ability to foster data sharing within their existing network in order to help verifiers make better fraud and credit risk decisions. One important distinction here is between data sharing for the purpose of protecting the end customer (this is what fraud data consortiums like **Plaid Beacon** are focused on) and data sharing to protect financial services providers from credit and first-party fraud risk (this is the data that typically falls under FCRA).

- **Consumer Control** – If congresspeople and senators in the 1960s could have foreseen how technology would develop over the next 50+ years, I suspect that they would have written the Fair Credit Reporting Act a bit differently. Specifically, I would guess that they would have done what many regulators and consumer advocates are pushing for today – making consumer permission the foundation of all data collection rules and best practices. The winners in the identity issuer race will make consumer permission and control the centerpiece of their digital identity strategy.

Patience

Digital identity is not a new concept. Nor are the criticisms of our current, sub-optimal approaches to identity verification and fraud management.

Paradigms don't shift overnight.

But eventually – when the weight of evidence becomes overwhelming – they do, and when that happens, we learn to think about these problems in entirely new ways.

I think we're getting close to that moment with digital identity.

About PLAID

Plaid helps companies reduce fraud and win more trusted users. With one of the fastest, one-click experiences on the market, **Plaid Identity Verification** is trusted by hundreds of leading companies across the lending, wealth, proptech, e-commerce, and banking industries to simplify onboarding, mitigate risk, and verify users' identities in seconds.