A GREAT DIGITAL IDENTITY SOLUTION IS ONE YOU CAN'T SEE

By Sushmita Banerjee, Tanwee Misra, Saipriya Sen Kohli, Michael Marcus, Michael Coden, and Gary Curtis

IDENTITY SOLUTIONS ARE AN integral part of the digital experience—and consumers want nothing to do with them. By authenticating users, these platforms keep fraud at bay, boosting trust, clicks, and sales. But they often require consumers to jump through hoops—creating unwieldy passwords, for example, or entering verification codes from a second device. The seamless convenience consumers expect online is now a trip to the dentist.

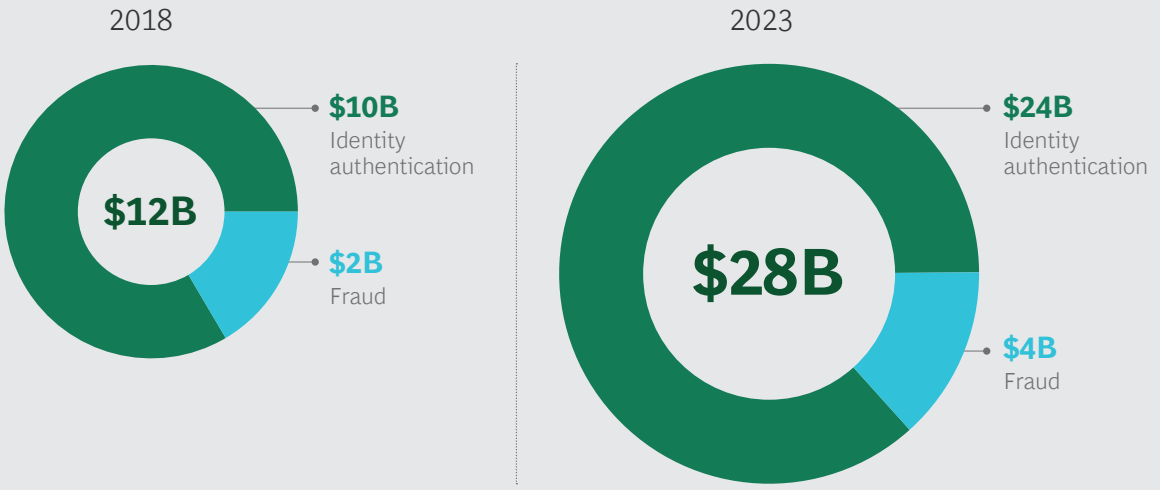
As a result, many digital identity solutions aren't as efficient, effective, or commercially successful as they could be. Consumers often decline to use more secure, but more onerous, features like multi-factor authentication. Meanwhile, a number of large businesses—including some of the household names of the digital era—have opted to go their own way, creating proprietary identity platforms.

No solution—whether homegrown or off the shelf—will truly succeed unless it is designed with consumer preferences and behavior in mind. This means using data and technology in a way that lets authentication operate invisibly in the background—just the way consumers like it. This isn't easy to do. The solution must access the right identifying information at the right time, leverage a flexible data infrastructure (one that brings together different types of structured and unstructured data), and call on sophisticated capabilities in artificial intelligence and machine learning. But this holistic approach to digital identity—bringing simplicity to consumers, security for businesses, and success for the providers who get it right—is achievable.

A Clear Need but No Clear Leader

As connected devices proliferate and digital transactions multiply, we expect the market for identity authentication and fraud solutions to boom, increasing from $12 billion in 2018 to $28 billion in 2023. Identity authentication will be an increasingly important component of that market. (See Exhibit 1.) Robust front-end verification—ensuring that the person initiating a digital transaction is who they say they

EXHIBIT 1 | The Market for Identity Authentication and Fraud Solutions Will Reach $28 Billion by 2023



Source: BCG research and analysis.

are—can help minimize fraud by keeping out bad actors.

This gatekeeping is essential if consumers are to put their trust—and their dollars—in online transactions. In the digital era, nothing is certain except death, taxes, and data breaches, and many of those breaches expose personally identifying information, such as passwords, social security numbers, and credit card data. In the first six months of 2018, according to the Gemalto Breach Level Index, some 3.25 billion records were compromised in the US alone, a 356% increase over the same period in 2017. Effective authentication can take big bites out of both direct fraud (such as unauthorized money transfers) and downstream fraud (the billions of dollars lost each year to transactions that utilize data compromised in a breach).

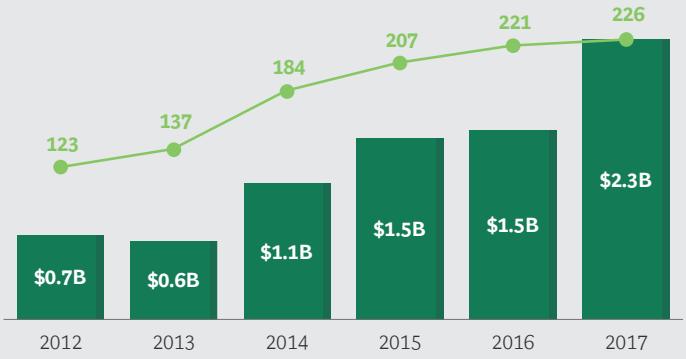
Not surprisingly, many players want to lead the gatekeeping. Established identity solutions providers and startups alike are building capabilities and pursuing patents and acquisitions. In 2017, there were 226 identity deals funded via the private equity market, according to CB Insights—up from 123 in 2012. (See Exhibit 2.)

Yet even with all the investment and interest, the market still lacks a clear leader. Three significant challenges explain why this is the case:

- **Solutions place unwanted burdens on consumers.** Current solutions ask users to play an active role in protecting and verifying their identity. But common practices like multi-factor authentication, security questions, and frequent password changes are burdensome—and many users are just saying no.[1] In a 2017 Gemalto survey of more than 10,000 consumers, 56% said they use the same password for multiple online accounts. And 41% declined to use two-factor authentication when offered the option for their social media accounts. Yet while consumers may have a laissez-faire attitude toward their own identity hygiene, they are decidedly less forgiving of the businesses they use. In the same Gemalto survey, 62% of respondents noted that businesses are responsible for data security, and 70% said they would part ways with a company if it experienced a data breach. (See Exhibit 3.) This inconsistency—users demanding security but not tightening their own habits—is important. Identity solutions must account for it, but today they are falling short.

- **Providers use identifying data in a suboptimal way.** In the offline world, certain mainstay types of data—including driver's licenses, passports, social security or tax ID numbers, credit histories, and knowledge-based ques-

EXHIBIT 2 | Dealmaking Surges as Players Build Capabilities



Growth rate (CAGR)

Number of identity-related deals **13%** ↑

Private equity funding ($B) **27%** ↑

Sources: CB Insights; BCG analysis.

tions—have long been used to verify identities. But as technologies evolve and digital transactions increase, new types of data are becoming valuable for proving identity. These include biometrics (such as fingerprint patterns and face and retina scans), IP addresses, device IDs, geolocation data, and even behavioral analytics (recognizing, for example, the typing style of a user). Crucially, these data types can facilitate the kind of automated, frictionless authentication process that consumers prefer, because they don't require significant effort from the user (looking into a camera for a face scan is a lot easier than remembering the name of your seventh-grade math teacher). The problem is that this data is typically available from just a handful of sources. So many providers of identity solutions aren't accessing and integrating it into their platforms—and verification is not as seamless as it could be.

- **Providers lack cutting-edge technology—or aren't able to use it effectively.** Artificial intelligence and machine learning can greatly simplify—and, crucially, automate—identity authentication. And they can do so while improving accuracy and security. But these technologies can't work in a vacuum. Algorithms need to be trained, and that requires scale: the more users on a platform, and the more data points to work with, the more efficient and effective the solution. The market presents a paradox. The startups that have promising technology often don't have sufficient scale, while the established players that do have the necessary scale often don't have the innovative technology. Either way, compelling advances in identity authentication aren't utilized to their full potential.

These challenges are holding back identity solutions—to the point where some digitally focused businesses are taking matters into their own hands. Amazon, Apple, Facebook, Google, and Microsoft are among the companies that are bypassing providers and developing homegrown solutions. Yet these same challenges also create an opportunity. A provider that understands the pain points and can navigate around them could create a solution that works for all stakeholders—one that is seamless for consumers, efficient and effective for businesses and governments, and a differentiator for its creator.

The Pillars of a Robust Identity Solution

To create a seamless, efficient, and differentiating experience, solutions providers—startups and established players alike—need to rethink their strategy. They need to evolve their solutions to align with consumer preferences and make the most of the data and technologies relevant to digital identity. This means embracing five key practices:

- **Build solutions around actual consumer behavior.** Consumers have

made it clear that they don't want to jump through hoops to verify their identity. They just want to see their Facebook feed or complete a purchase. By incorporating the right mix of data and technology, providers can create a more seamless, even frictionless, user experience. But a deep understanding of customer behavior—specifically, the behaviors that are natural for users—should inform every phase of solution design. One idea is to adopt the concept of human-centered design, which many technology companies are already putting to use in creating new products, platforms, and user interfaces. (See "Take Control of Your Digital Future," BCG article, May 2018.) The hallmark of this approach is making detailed observations of how users interact with systems, and adjusting designs accordingly. Companies put prototypes in front of users, scrutinize responses, make any necessary tweaks, and repeat the process—in fast, iterative cycles—until design and preferences align.

- **Ensure access to the right data at the right time.** By utilizing a variety of data—such as mobile phone location data, biometrics, and behavioral analytics—identity solutions can do more of their work invisibly, in the background, reducing or eliminating the burden on consumers. But accessing the right data—at the scale and speed needed to make fast, accurate determinations—isn't easy. Many of the most useful types of data—such as biometrics and device IDs—are not widely available. And some identity players have already acquired key sources, limiting availability even further. Would-be leaders must move fast to identify the most valuable types of data and to ensure—through partnerships or acquisitions—their access to it.[2]

- **Integrate data with robust capabilities and infrastructure.** Advanced analytics enable solutions to triangulate all the different sources of data to authenticate identities. But it's not as simple as flipping the switch on an algorithm. Working with many data types and determining identity with a high degree of precision requires the right mix of technology and processes. First, providers will need to invest in artificial intelligence and machine learning capabilities. At the same time, they'll need to understand that AI and ML—and the analytics built around them—aren't perfect right out of the box. Sometimes the model will be wrong or won't have enough information to authenticate with certainty. So providers will also need operational processes in which humans adjudicate and feed intelligence back into the model (as the systems "learn," the amount of human intervention decreases and the level of automation increases). Providers will also need a flexible infrastructure, one that uses APIs to integrate—with plug-and-play ease—external sources of data, as well as new sources that may become valuable in the future. Such flexibility will likely require significant

EXHIBIT 3 | In a 2017 Gemalto Survey of More Than 10,000 Consumers Worldwide . . .

56%
said they use the same password for multiple online accounts

41%
declined to use two-factor authentication when offered the option for their social media accounts

62%
said that businesses are responsible for data security

70%
said they would part ways with a company if it experienced a data breach

Source: Gemalto survey (https://www.gemalto.com/press/pages/majority-of-consumers-would-stop-doing-business-with-companies-following-a-data-breach-finds-gemalto.aspx).

investment and effort, with open, cloud-native architecture replacing the largely inflexible legacy IT systems. But providers that take these steps will see a giant leap in their ability to use new forms of data—and to seamlessly authenticate identity.

- **Sharpen the focus via use cases.** Industry- and country-specific requirements make a one-size-fits-all identity solution unlikely. Banks, for instance, must satisfy regulatory standards that don't apply to retailers. But this doesn't mean that providers need to limit their aspirations to specific markets. Instead, they can—and should—build on their solutions and experience to broaden their reach over time. The idea is to take a use-case approach. For example, a provider might develop a laser-focused solution for a very specific need, such as authenticating employees entering a building or bank customers opening a new account. Then, leveraging the lessons learned, the provider could generalize—and expand—that solution across industries and even geographies, if the regions have similar legal and regulatory frameworks and data sources. The use-case approach opens the door for specific types of businesses—such as financial institutions—to become key players in identity solutions. In some countries, the public sector could also assume a major role, working with providers, for example, in the development of federated identity for government services—whereby a single sign-on is used across multiple organizations. In all of these permutations, the key advantage is that providers can place bets strategically, prioritizing use cases that play to their strengths—and building from there.

- **Consider new trends and their potential impact.** Digital identity will continue to evolve as new technologies, regulatory structures, and ideas gain traction. Recent developments include the European Union's General Data Protection Regulation (GDPR); India's Aadhar program, which assigns every citizen a digital identifier; the California Privacy Act; and China's cybersecurity law, which puts stringent requirements on the transfer and use of personal data outside that country. Meanwhile, concepts like decentralized identity and self-sovereign identity, which put control of personally identifiable information back in the hands of individuals, are emerging. Each of these developments—and those yet to come—may have an impact on what businesses and governments require from identity solutions and on how consumers use those solutions. By staying on top of the trends and the regulations, providers can evolve their solutions smartly—and successfully.

Digital identity is a fast-moving space in which technologies, data, rules, and preferences are in constant flux. But one thing is certain: the most successful solutions will provide a user experience that's tailored to how consumers are actually likely to behave. For providers, that means designing solutions with the consumer's perspective—and preferences—always top of mind. It also means utilizing data, technological capabilities, and processes in a holistic way, investing in and applying the mix that simplifies yet enhances authentication. This kind of seamless, secure identity solution will be a boon for consumers and businesses—and a bane for fraud.

Notes

1. Complicating the challenge related to the burden on consumers is the fact that multi-factor authentication is often misunderstood or misapplied. There are three categories (or "factors") of authentication data: something you know (such as a password or challenge answer), something you are (such as a fingerprint), and something you have (such as a smart card or mobile phone). Multi-factor authentication must involve at least two of these categories. A solution that relies on multiple elements from only one category (such as a password and answers to challenge questions) is not true multi-factor authentication—and is not nearly as secure.

2. Although they may not possess all of the new types of identity data, financial institutions tend to have the most complete data sets (at least among non-government entities). This presents a unique opportunity for these players to partner with retailers, airlines, and other businesses to authenticate consumers.

About the Authors

Sushmita Banerjee is a partner and managing director in the New Jersey office of Boston Consulting Group. You may contact her by email at banerjee.sushmita@bcg.com.

Tanwee Misra is a project leader in the firm's New York office. You may contact her by email at misra.tanwee@bcg.com.

Saipriya Sen Kohli is a senior knowledge analyst in BCG's New York office. You may contact her by email at kohli.saipriya@bcg.com.

Michael Marcus is a senior advisor in the firm's San Francisco office. You may contact him by email at marcus.mike@advisor.bcg.com.

Michael Coden is a BCG Platinion managing director in the firm's New York office. You may contact him by email at coden.michael@bcg.com.

Gary Curtis is a senior advisor in BCG's San Francisco office. You may contact him by email at curtis.gary@advisor.bcg.com.

Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.