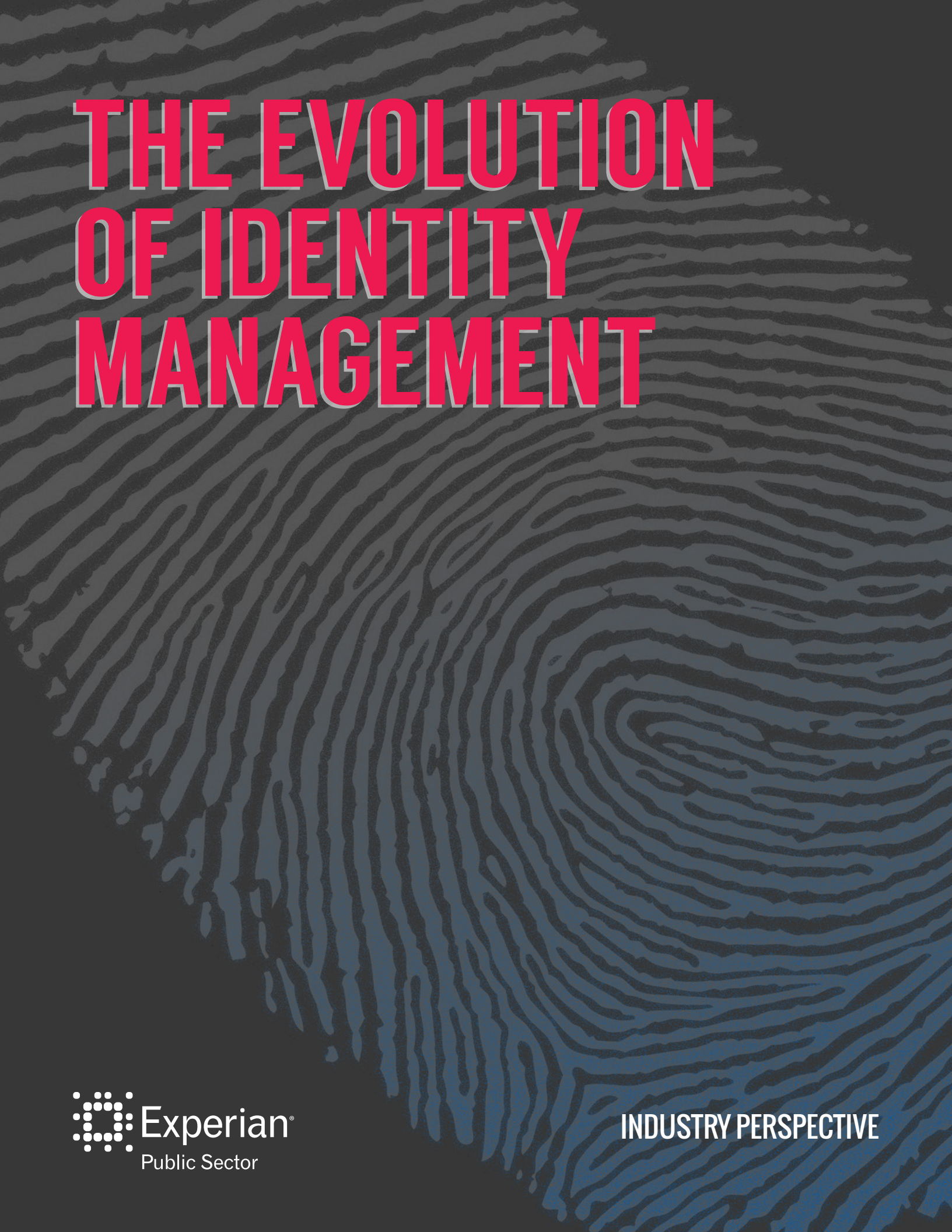
THE EVOLUTION OF IDENTITY MANAGEMENT



Experian®
Public Sector

INDUSTRY PERSPECTIVE

EXECUTIVE SUMMARY

Given the mounting threat of cyberattacks, coupled with a proliferation of information now accessible online, multilayered identity management systems are more important than ever to an agency's security infrastructure.

Fortunately, most organizations understand the necessity to protect online information by creating stringent verification processes for users. Simply ensuring that the right person is accessing your information, however, is no longer enough.

Today, agencies must build strategies that reflect the evolution of identity management and look beyond identity verification at the point of login. Considering this concept, identity management strategies must:

- Ensure that identification processes are appropriate to the target demographic
- Leverage diverse data sets to transform verification processes
- Evolve over time as agencies and user needs change
- Adhere to credentialing regulations without decreasing user satisfaction

To help us understand how agencies can modify their identity management strategies to fit evolving market demands, we spoke with Kolin Whitley, Director of Fraud and Identity Solutions at Experian, a global information services provider that offers a suite of identity-proofing tools to both public and private sectors. He explained how identity management is changing from a single sign-on process to a constantly evolving relationship between agency and user.

MORE THAN LOGGING IN

Identity management is no longer a matter of ensuring one-time verification. "It's not just knowing who that person might be at one point in time but considering the risks associated with that identity profile and being able to manage those risks throughout a customer lifecycle," Whitley explained. Your credentialing processes should consider the long-term relationship between a user and your services. As a user becomes more familiar with—even reliant on—your agency's services, the way he/she accesses and uses information will change significantly.

For instance, an extensive credentialing process may be appropriate for a first-time user. After all, you want to authenticate your users and ensure they are accessing your agency's data appropriately. However, if that person logs on and continues to use your online services properly, his/her credentialing process for each subsequent action should be minimized.

A cumbersome process is likely to discourage a user from optimizing your data due to fatigue. Additionally, providing an impersonal experience can sever the trust built between an agency and its consumers. In either scenario, a burdensome authentication system risks decreasing your agency's ability to effectively engage and serve the public.

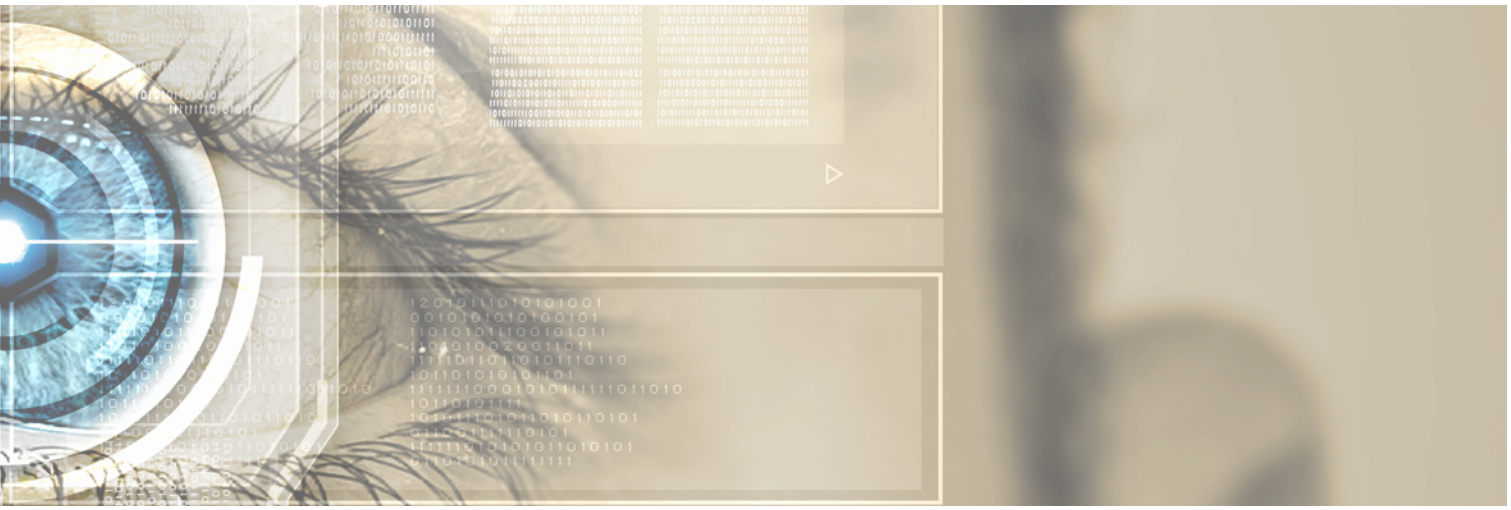
KNOWING YOUR AUDIENCE IS KEY

Like any relationship, your user-agency connection will develop only if you understand a person's background, habits and interests. "It's important for us to consult with agencies to make sure that they understand the demographic that they're dealing with, and that there may be certain challenges based on that unique demographic," Whitley said. A person's personal history will heavily influence their preferences and ability to establish a credentialed identity within your system. Therefore, the composition of your user-base should be a guiding consideration in your identity management strategy.

Basic demographic information such as the age, location and gender of your users can come from a range of sources. In some cases, getting to this unique information may require collaborating with a data and analytics provider like Experian. Alternatively, your agency may already know the makeup of its primary users via data from its online traffic.

This online history can also provide other valuable information about your consumers. To make the user experience as comfortable as possible, you must look beyond basic demographics to understand how your audience interacts with your agency. Challenge your strategist to consider the actions and preferences of your users: How frequently do they access sensitive information? Do they generally log in via a computer or from a variety of mobile devices? Do they have an elementary or complex understanding of privacy concerns? Finally, when users are accessing your services, are they able to get to the information they need or are heavy credentialing processes impeding their progress?

Determining the profile of your users will set the stage for transforming your identity management strategy; your next step is to analyze that information and its implications. For instance, if you learn that the majority of your users are in their early twenties, you will want to assimilate that fact into your credentialing methods. How so? Since younger users may have limited experience with personal finances, you may want to minimize questions that rely on credit history for authentication. You may also need to focus on streamlining credentialing processes across multiple platforms, as younger users are likely to use a variety of mobile devices for access.



FINDING THE RIGHT BALANCE

There is no one-size-fits-all template of credentialing requirements. Your appropriate identity management strategy is dependent not only on your user base, but also on your agency's particular mission, risk tolerance level, and regulatory environment. Each of these components will shift your identity-verification tactics, making them more extensive when necessary and less invasive where possible.

"It's really up to the agency to make those hard business decisions of where they want that threshold to be and where they want to strike that balance," said Whitley.

Every facet of your agency, including its credentialing process, should serve your mission. Your mission is not static. It manifests in different ways over different mediums and processes over time. Your identity management tactics should be equally diverse and adaptable.

"Every agency has a slightly different mandate that they're trying to meet," Whitley explained. "Being able to work with application providers who have the flexibility to provide a customized approach helps them tremendously as they work through that mandate."

In many instances, your mission is best served by encouraging as many users as possible to access your information. In those scenarios, a light credentialing process is most appropriate to avoid impeding users from engaging with your agency. In other cases, however, advancing your agency's cause may require strictly securing data to ensure that only those users who can and should appropriately use it have access to it. For instance, departments should deploy a stringent identity authentication process to protect large, complex data sets that can be easily corrupted by fraudsters or novice users.

Security is clearly a primary concern for many agencies. However, as noted by Whitley, "It doesn't make a lot of sense to have a user go through an expensive and, in some cases, perceived invasive form of identity verification just to reset a password." Some processes need to be safeguarded better than others. The ideal identity management strategy will reflect not only the risk tolerance of your organization at large, but also the unique risks associated with particular access scenarios. Whitley explained how Experian helps determine this strategy: "We work and engage with the client to come up with the best mix of risk strategies that will optimize the performance of the product while still maintaining that level of security."

Finally, considering the environment in which your agency operates is also important. Regulatory standards can safeguard or inhibit your ability to service these users. "The challenge that we encounter quite often is that an agency has a directive requiring them to authenticate users accessing their applications," said Whitley. "But at the same time, they are trying to balance the fact that these users do need to access those applications."

Regulations may require stricter credentialing processes than you might otherwise find appropriate for a specific user action. In these instances, helping to alleviate credentialing burdens while remaining compliant with your regulatory environment should also be part of your identity management strategy.

USING DATA CREATIVELY

In order to adhere to your mission, risk and regulatory constraints without impeding users from accessing your services, Whitley suggested rethinking the way you use your data to credential users. Once you determine what you have to verify about each person and for each process, leverage your data to make the process of credentialing less intrusive and complex.

"We have an extensive collection of data across institutions that is coupled with public and private sources," Whitley pointed out. "It really allows us to come up with a mix of strategic questions that can be used effectively by our clients."

Whitley offered an example of how this might work. "An organization may decide that it is not appropriate to gain consent from an end user in order to use Fair Credit Reporting Act regulated financial data," he explained. "We can quickly deploy a strategy that can use alternative data and challenge the user with a series of less invasive questions about his or her demographic and non-financial bases data history."

These questions are less intrusive and therefore less likely to dissuade a user from accessing your services. At the same time, they confirm necessary information — a person's established data footprint — which allows your credentialing process to remain consistent with regulations.

This tactic can also be used to simplify the process of credentialing for your user. Asking for verification information that may not be readily on-hand may impede a user from logging on to your website. Similarly, asking a range of questions that are seemingly unrelated or simply too extensive can dissuade a user from taking the time to finish the credentialing process.

"You have to come up with that mix of data asks that are in context, and most appropriate for their application," Whitley explained. Rather than asking five questions to verify one aspect of identity, consider a different data set that might confirm a person in fewer steps with greater cohesiveness between questions. By considering all the disparate information that can be used to identify a person, Experian creates a credentialing process that is fluid, consistent and simple.

> "You have to come up with that mix of data asks that are in context, and most appropriate for their application."
>
> **— Kolin Whitley,**
> Director of Fraud & Identity Solutions, Experian

ENSURING EVOLUTION

Once you have streamlined your credentialing process to tackle the needs of your users and your agency, it's important to consider how your identity management strategy will adapt to new challenges. Remember that credentialing is a relationship rather than a one-time login.

"It's important to look at how an identity may change over time or new risks that might be introduced post–initial ID proofing," said Whitley. As your user relationship evolves, your identity management system must adapt as well.

Whitley advised that, "Organizations really need to look at providers that not only have a track record in the identity management space, but also have a roadmap moving forward that indicates a commitment to creating those unique strategies specific to the public sector." In other words, you should ensure that the authentication and credentialing strategies you create will be monitored for efficacy and updated when needed.

Experian's model of service provides ongoing support to ensure that your identity management strategy can adapt to future user, regulatory and agency needs. The Experian team works with key stakeholders to monitor the progress of a strategy, even after it has been deployed. "It's not just a turnkey solution that we drop in and walk away from," Whitley said. "We continually consult, monitor performance and make adjustments as needed."

In order to ensure that a strategy remains consistent with user demands, Experian develops targeted indicators to monitor system performance. Along with these targets, "We have a very extensive and granular reporting mechanism that can look at the performance of each question, how it performs against our benchmark, and then make adjustments," Whitley said.

Experian's modular approach to identity management makes this adjustment possible. "What provides us a distinct opportunity and unique position in the marketplace is our agility, and our ability to bring in different processes and information," said Whitley. "The whole point is that you're giving those options to agencies so that they can pick and choose the type of authentication that they want to use based on their application and scope."

Agencies will eliminate, modify and accrue specific applications well beyond initial deployment of their identity management system. Concluded Whitley, "We must evolve from an identity access management position to an identity relationship management position. We must use our data to address the needs and context of our end users over the lifetime of our relationship with them."

ABOUT EXPERIAN PUBLIC SECTOR

Experian public sector integrates predictive data and analytics to provide greater insight into decision performance to help agencies and organizations keep pace with changing priorities. By applying expert consulting and analytical tools to convert data into valuable business decisions, we uniquely positions public professionals with a solutions-based approach to be better prepared to make decisions, manage programs, protect citizens and deliver results to complex missions.

Contact us today at 1 (888) 414-1120 to learn more or visit us at www.experian.com/publicsector

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 150,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C. with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to Hannah Moss, Research Analyst, GovLoop, at hannah@govloop.com.

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com

Twitter: @GovLoop

1101 15th St NW, Suite 900
Washington, DC 20005

Phone: (202) 407-7421 | Fax: (202) 407-7501

www.govloop.com
Twitter: @GovLoop