Numerous technological elements are quickly maturing to the point where widespread availability of secure and cost-effective identity measures is already here or coming soon. Consider biometrics on mobile devices. Not too long ago, biometric access was only available on high-end smartphones. Its security was also a question, as people quickly uncovered easy ways to defeat its. Soon, as the number of smartphones with biometrics ramps us and the security becomes increasingly secure, highly secure biometrics will be a powerful authentication device in the hands of billions of people. Other pieces of the digital identity technosphere are similarly coming into place, from total global internet coverage to AI-powered fraud detection systems, from 5G access to next-gen sensors with impeccable accuracy. With so many technology options, though, what is the best way to create legal structures that carefully consider the capabilities, use cases, existing regulations, consumer requirements and international cooperation? While each country will have to determine its own path, at least the Guidance provides a common starting point. Thus, while still only a draft, the Guidance offers powerful insight for what is coming next in terms of digital identity. Digital ID systems — digital ID assurance frameworks and standards Fortunately, there are powerful international standards bodies that are developing technical standards for digital ID; the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are working on updating identity, IT security and privacy rules. Depending on the use case, these technical standards can offer the necessary level of confidence, the higher "levels of assurance" that meet the lofty standards required by regulated industries for handling sensitive information. As the FATF recommends financial institutions apply a risk-based approach, conducting Customer Due Diligence (CDD) will require determining "an appropriate level of trustworthiness" for digital ID systems: What level of assurance does the system technology, architecture and governance provide in terms of reliability and independence? Is the level of assurance appropriate to the risk level of potential money laundering, terrorist financing, fraud and other risks? Digital identity systems present a potential danger in introducing new risks. Cyberattacks, data breaches and massive identity fraud are all examples of new forms of risks that require consideration. Just as technology helps scale compliant solutions, it can amplify the scope and speed of attacks. If the technical standards and implementation procedures are at a sufficiently high level, these risks will be minimized. Significant cyber risks exist for all types of businesses and processes and require concentrated efforts to keep them contained. As new systems might irrevocably change the risk parameters, a thorough review of the associated risk and associated policy revisions in conjunction with digital ID is good practice. In many cases, the risk level will drop, as digital ID systems continue to advance and become robust, secure and trustworthy. Reexamining risk scenarios makes sense for both regulators and regulated entities. Changing the risk equation One advantage of using digital identity processes is the ability to easily integrate other technologies into the system. Advanced data modeling and analysis is readily available, as the data is already in digital form. Monitoring and reporting are more seamless, as the native format is convenient to manage and transform. Account access is more tightly controlled, as biometrics and digital profiles improve security measures. When it comes to improving financial inclusion, having a flexible approach to assurance levels can help unbanked people get into the formal banking system. The risk of money laundering is generally less with lower value accounts; thus, having the same strict standards for

all accounts is neither necessary or helpful. As Trulioo COO Zac Cohen, states, “assurance levels are key, and by providing structure and flexibility into how we can manage assurance levels (and still be in compliance), it opens the doors for greater financial inclusion everywhere.” One digital ID to rule them all? The digital identity and document verification market is forecast to grow to $15 billion by 2024. There are numerous solutions from various vendors, with different jurisdictions specifying divergent requirements. As the technology improves, new use cases become palatable and the market expands further. While having multiple options does have its benefits, it also causes confusion in the marketplace and internal havoc as organizations try to optimize and synchronize processes. The Guidance provides a high-level overview of how to coordinate standards and solutions for better digital identity for all. As Cohen puts it, “it’s a holistic look at how can we collaborate to a standard that makes sense regardless of the use case or scenario.” Trulioo looks forward to helping create this flexible digital identity standard that grows the market, provides security and compliance, and delivers on the needs and requirements of consumers, business, and government. It aligns with our vision, the consortium view of identity, where different technologies and solutions work together to build a better world for us all. As Trulioo CEO and founder Stephen Ufford states, “a consortium view of identity has been, and will continue to be, the way to go forward.”