Better Identity Coalition Releases Best Practices for Responsible Use of Verifiable Digital Credentials

New framework establishes "rules of the road" to protect privacy while enabling secure, convenient digital transactions

WASHINGTON, D.C. — October 28, 2026— The Better Identity Coalition today released a set of best practices designed to ensure that the emergence of new digital counterparts to the paper and plastic credentials that governments issue today do not lead to a future where people are expected to share their identity every place they go online.

"**Verifiable Digital Credentials - Best Practices for Organizations Requesting and Using Identity Data**" establishes a set of voluntary guidelines to ensure that new government-issued verifiable digital credentials (VDCs) such as mobile driver's licenses (mDLs) improve privacy, security, and convenience, without leading to inappropriate requests for ID.

The Best Practices are designed to establish clear "rules of the road" that preserve individuals' ability to interact anonymously or pseudonymously online while enabling the use of trusted digital identity when there is a legitimate legal, regulatory, security, or business need.

"As digital credentials start to emerge, it is important to ensure that their arrival does not lead to a world in which individuals are expected to share their identity every place they go online," said Jeremy Grant, Coordinator of the Better Identity Coalition. "This set of Best Practices is intended to address these concerns – by establishing guidelines that everyone in the digital identity ecosystem can follow and use as a tool to restrict inappropriate or overly invasive requests for identity information online."

At the heart of the framework is the principle that the emergence of digital credentials should not materially diminish an individual's ability to remain anonymous or pseudonymous online. When identity information is needed, organizations should request only the information necessary for the specific transaction. The framework also makes clear that having a legitimate reason to collect identity information for one transaction does not justify collecting it for unrelated interactions.

To translate those principles into practice, the Best Practices identify specific use cases where VDCs can appropriately be used. These include:

- High-risk transactions – largely associated with financial services, health care, and government benefit programs – where there are legal or regulatory requirements to determine the identity of an individual, or in some cases, validate something about them (i.e., that someone is over 21 or a resident of a particular state).

- Transactions where there is no legal or regulatory requirement to collect and validate identity data but where the risk model is such that service providers do not make a product or service available online because there is a business need for that provider to validate identity data– and so that service provider has traditionally asked to see an ID.

For each use case, the framework identifies the identity attributes that are appropriate for an organization to request.

Importantly, the Best Practices also flag cases where requests for any data from digital ID should be restricted, including using digital identity or age verification to deliver targeted advertising or using VDCs like cookies to track individuals' behavior online.

The Best Practices also call on organizations using data from government-issued VDCs to embrace fundamental privacy protections, including data minimization, transparency, purpose limitation, prohibitions on selling or sharing VDC data except where required by law, protections against tracking, and mechanisms allowing individuals to correct or delete their information. Consumers should also have an alternative path when they do not want to use a digital credential.

This initiative grew out of a Better Identity Coalition workshop that brought together approximately 60 representatives from privacy and civil liberties organizations, consumer groups, digital wallet providers, identity technology companies, major online service providers, and governments.

The Coalition views this initial release as a starting point and expects the Best Practices to evolve as organizations deploy digital credentials and new use cases emerge. The Coalition will maintain the Best Practices and plans to consider updates based on stakeholder feedback and implementation experience.

The full Best Practices can be downloaded here.

Here's what stakeholders have to say:

"Our digital license and identification program is an important step toward making identity services more convenient and accessible. The Better Identity Coalition's Best Practices document can be a valuable guide as we continue to build a program that prioritizes security, privacy, and the needs of the people we serve," said Georgia Department of Driver Services (DDS) Commissioner Angelique B. McClendon.

"Mobile driver's licenses and digital IDs should deliver a more convenient and secure experience, all while enhancing users' privacy," says David Brudnicki, Senior Director of Wallet Services at Apple. "This principle has guided how we've designed IDs in Apple Wallet, and we support the Better Identity Coalition's work to establish clear guidelines and responsible practices that protect people's privacy as digital credentials become more widely adopted."

"The opportunity for verifiable digital credentials to change how identity is trusted is real, but so is the responsibility to get them right," said Richard Grape, Senior Director of Market Transformation, LexisNexis Risk Solutions. "Done well, they make proving identity safer and more accessible. The Better Identity Coalition's best practices help clarify when asking for identity is appropriate and when it is not. In Arizona, LexisNexis Risk Solutions is proud to support the issuance and verification of the nation's first digital birth credential (dBC), a model that can improve assurance, reduce friction, and deliver convenience at scale."

“Verifiable digital credentials like mDLs give us a more secure, privacy-preserving way to prove who we are online, while offering businesses a much stronger signal of authenticity than a snapshot of a plastic card in the age of cheap and convincing deep fakes. The Better Identity Coalition’s best practices give relying parties the guidance they need to start accepting digital credentials with confidence,” said Will Wilkinson, Director of Government Affairs, Persona.

“Verifiable digital credentials can strengthen trust, help prevent fraud, and give individuals more control, but they also introduce risks,” said Tim Cappalli, Senior Architect, Identity Standards at Okta. “The Better Identity Coalition’s best practices enable responsible use of these credentials, so people can prove who they are online without sharing more information than necessary. Okta is proud to contribute to this effort in support of our mission to free everyone to safely use any technology.”

“These best practices further support the guiding principles of the ISO/IEC 18013-5 standard that balance privacy, security, interoperability, and trustability without sacrificing one for another,” said Ian Grossman, President & CEO, AAMVA

About the Better Identity Coalition

The Better Identity Coalition is collaborating with policymakers to improve digital security, privacy, and convenience for everyone. The coalition brings together leading companies to promote education, collaboration, and better solutions to protect identities online.

Together, we’re seeking innovative ways to empower Americans to take control of their identities and conduct their online business safely and securely.

Launched in 2018, the coalition is an initiative of the Center for Cybersecurity Policy and Law, a nonprofit dedicated to working with policymakers to advance cybersecurity initiatives.

Media Contact:
Tonya Riley
TJRiley@Venable.com
202.344.4528