Strawman v0.1 – Verifiable Digital Credentials Voluntary Code of Conduct

I. Introduction

a. Governments are increasingly offering their residents the option of storing a digital counterpart to the paper and plastic credentials government agencies issue in digital wallets. In the United States, state governments have been at the forefront of digital credentials with new mobile driver's licenses (mDL) initiatives, however, a variety of Federal, state, and local agencies are considering launching similar initiatives that might encompass authoritative government credentials including passports, social security cards, and birth certificates. Together, these digital IDs represent a new class of verifiable digital credentials (VDCs) that will likely transform the ways that people in the United States prove their identity, both in person and online.

b. VDCs have the potential to improve security, privacy, usability, and inclusivity for individuals and business if they are designed, deployed, and used responsibly. However, the introduction of VDCs, specifically government issued ones, also brings the possibility that they could erode security, privacy, and civil liberties. Among the top concerns is that, by making it easier than ever for individuals to prove who they are online, companies and government agencies will start to ask for ID for use cases where they rarely – if ever – did so before. And in doing so, it would significantly change the balance of power in terms of what is expected of individuals to allow them to engage and transact online.

   Since the dawn of the Internet, the ability to be anonymous or pseudonymous online in the vast majority of one's interactions has been a core feature of the Internet. An exception has been in a set of high-value and/or 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). There are also a number of 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 or attributes - and so that service provider has traditionally asked to see an ID.

   As VDCs start to be used in the marketplace, 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.

   Likewise, there are concerns that VDCs could be used as a way to augment or replace cookies and other technologies that are currently used to track behavior online. VDC standards have been specifically architected to ensure that

individuals can assert their ID – and online service providers can validate identity or attributes – without enabling new forms of tracking. It is important to ensure as VDCs are implemented that they are not used by some actors to enable new ways to track individuals.

c. In other countries, governments are setting rules to govern who can ask for proof of ID online, and in what circumstances. In the U.S., however, neither Federal nor state governments have focused on this issue. This voluntary Code of Conduct is intended to address these concerns – by establishing a set of rules that digital wallet providers and others in the digital identity ecosystem can pledge to adhere to, and use as a tool to restrict inappropriate or overly invasive requests for identity information from online service providers. The goal is that, by proactively setting rules of the road for the use of VDCs, this Code can mitigate the risks involved with new government digital credentials while ensuring that the benefits of improved security, privacy, usability, and inclusivity are fully realized.

II. Overview of the Code of Conduct

a. **Purpose**

This Code of Conduct aims to set a high bar for security, privacy, usability, and inclusivity associated with the use of VDCs, by:

- Introducing a set of core principles to govern VDC use
- Defining core use cases and attribute bundles where online service providers may ask for validated identity and/or attributes
- Outlining use cases where a request for validated identity and/or attributes is inappropriate and should be restricted

Companies and organizations that pledge to adhere to the code will then be empowered to restrict or limit requests for validated identities and/or attributes that are outside the scope of the Code.

In doing so, the Code seeks to preclude scenarios that could lead to gross overuse of digital identity and/or activities with regard to VDCs that could erode the ability to be anonymous or pseudonymous for many online interactions, or otherwise cause harm.

b. **Scope**

The Code is initially aimed at digital wallet providers (also known as credential manager providers) and other organizations that play a role in verifying and validating identity for online service providers using government-issued VDCs.

While digital wallet providers are the primary focus, the Code may also be adopted by online service providers (also known as verifiers). In addition, the Appendix of this Code provides guidance and best practices to online service

providers around their use of VDCs. It is expected that verifiers who choose to adopt the Code will be organizations specifically called out in the use cases in Section VIII; and in adopting the Code, they will be pledging to use VDCs in accordance with the terms outlined in the use cases. Verifiers can self-select into the use cases that are most appropriate to their business or mission.

Likewise, this initial version of the Code focuses solely on laying out the policies that will govern use of VDCs. As such, it does not include any provisions to certify that organizations who have pledged to follow the Code are actually doing so, nor does it address issues around technical infrastructure that could be used to enforce the Code, such as a way for wallet providers to grant or revoke access tokens to online service providers seeking to access VDC data stored in those wallets. However, it is possible that future iterations or versions of this Code might address these issues, or that other organizations will seek to launch certification programs or technical infrastructure to complement and support the code.

III. How the Code was Developed

a. The Better Identity Coalition convened a workshop in March 2025 to discuss emerging concerns about potential overuse of VDCs, explore potential ways to address those concerns, and discuss whether there might be stakeholder interest in a potential third party, voluntary Code of Conduct as one way to address them. The event was conducted under the Chatham House Rule, and included about 60 attendees who came from a mix of privacy and civil liberties advocates, consumer advocates, digital wallet providers, other vendors in the digital identity market, and major relying parties from financial services, retail, and health care. The event also included a number of government officials.

   At the workshop, attendees reached a rough consensus that:

   - Some sort of “rules of the road” are needed as digital counterparts to government-issued identity credentials roll out
   - In the U.S., government is not likely to create these rules any time soon
   - It would probably be helpful for a third party to create a Code of Conduct that could fill this gap

   The workshop did not explore:

   - What would go into the Code (i.e., what use cases would be permitted or forbidden)
   - How it would be enforced
   - Who would develop and run it

b. Following the workshop, the Better Identity Coalition convened a small working group with representatives from wallet providers, privacy and civil liberties

groups, issuers, and relying parties. Based on their inputs, Coalition staff drafted a strawman of a Code for public release and feedback.

c. [Placeholder to describe what happened after that – release of strawman, feedback received, incorporation of feedback, and publication of v1 of the Code]

IV. Ownership and Maintenance of Code of Conduct

a. The Better Identity Coalition will retain ownership of the Code of Conduct, and will publish and maintain on its website a list of companies and organizations that have agreed to adhere to the Code.

b. As feedback on the quality and effectiveness of the Code emerges, the Better Identity Coalition will consider revising the Code to address this feedback and improve the Code going forward.

c. Beyond revisions to the Code itself, the Better Identity Coalition has established a process to consider the addition of new use cases and associated data bundles that will be permitted under the Code. Interested organizations can make a formal request by filling out the form at [insert link to be established]; the Coalition will consider the merits of each request and publish updates to the list of permissible use cases every 6 months.

Questions for reviewers:
What should the process to revise the Code look like?
How frequently should we add new use cases?
Is an every-6-months update sufficient? Every 3 months?
Do we need to specify more here in the Code in terms of criteria for approving new use cases (or modifying existing ones), or can we put it in the form (which we have yet to create)?

V. Target Scope and Application

a. This is a voluntary Code of Conduct, and as such, it is open to any entity that wishes (and considers the Code of Conduct relevant to its business or operations) to implement and adhere to. Implementation by any entity requires publicly committing to adherence to the code, and outlining how the code applies to that entity and its operations.

Questions for reviewers:
What would be the best way for an entity to do this? Could it be done, for example, by referencing the code in the entity's terms of service or privacy policy?
What other approaches would make sense?

b. Enforcement (in terms of using the Code to restrict certain requests for identity or validated attributes) is up to the discretion of the entity who has pledged to follow the code.

c. At present time, there is no certification of entities that pledge to adhere to the code – though we or another party may choose to create such a program in future years.

d. At present time, there is no technical infrastructure built to support implementation of the code (for example, a way to provision access keys to relying parties who want to access digital credentials for a purpose that is allowed under the code) – though we or another party may choose to create such a program in future years.

VI. Terminology and Definitions

a. Attribute
   - An attribute - sometimes known as a claim - is a quality or characteristic ascribed to someone or something. An identity attribute is an attribute about the identity of a subscriber (e.g., name, date of birth, address).

b. Credential manager
   - An application, hardware device, or service which securely stores, organizes, manages, and enables presentation of VDCs. Digital wallets, state mDL apps, password managers, and passkeys managers are examples of credential managers.

c. Digital wallet
   - A type of credential manager which typically holds VDCs and other digital representations of physical world objects

d. Identity Proofing
   - The processes used to collect, validate, and verify information about a subject to establish assurance in the subject's claimed identity.

e. Holder
   - The individual possessing the wallet and/or VDCs. This individual is typically the subject of the credential (aka, the person to whom the VDC was issued).

f. Issuer
   - The entity that issues a VDC- for example, a state motor vehicle department for a driver's license, or the Social Security Administration for the SSN.

g. Validated Attribute
   - An identity attribute can be said to have been "validated" if an organization has gone through a process or act of confirming that a set

of attributes are authentic, accurate and associated with a real-life identity.

h. Verifiable digital credential (VDC)
   - A cryptographically verifiable, tamper-evident assertion of claims about a subject, signed by an Issuer. VDCs are stored in a credential manager.

i. Verifier
   - The entity that cryptographically validates the authenticity and integrity of a VDCl. A verifier is typically, but not always, the relying party - also known as an online service provider.

j. Verifier service
   - The underlying platform or infrastructure service which enables a Verifier to validate a VDC. In many cases, a verifier service will be a product offered by a digital identity vendor who helps verifiers integrate with different VDCs.

Questions for reviewers:
What other definitions are needed?
Are there pre-existing definitions in other publications or bodies that we should use here, rather than create our own?

VII. Principles

a. The emergence of VDCs should not materially impact the ability of individuals to be anonymous or pseudonymous online.

b. VDC's have been designed specifically to preserve and enhance privacy, with the ability for individuals to choose to share only a limited subset of their identity information, and do so in a way that does not allow any party to track how or where an individual uses their VDC. Digital wallet providers and others in the digital identity ecosystem should design and use VDCs only in ways that embrace these features, with a focus on solutions that minimize the amount of data an individual is asked to present in online transactions.

c. There are a number of use cases where online service providers have a legal or regulatory requirement to collect and validate data on an individual's identity – either a full credential, or sometimes a subset of attributes associated with that credential – and use of a VDC for these purposes should be explicitly permitted, provided that the request is for a subset of identity data directly relevant to the requirement.

   For example, a bank is legally required to obtain the name, date of birth, address, and taxpayer identification number (TIN) from customers opening new accounts.

d. There are a number of use cases where there is no legal or regulatory requirement to collect and validate data on an individual's identity, but where:
   - The risk model is such that service providers do not make a product or service available online because there is a *[TBD – what terminology do we use to describe the threshold?]* need for that provider to validate an individual's identity, and
   - Most consumers would want the ability to access that product and service in a fully online environment, and would welcome the ability to do so rather than have to present their ID in person.

   Use of a VDC for these purposes should be permitted, provided that the request is for a subset of identity data directly relevant to the requirement.

   For example, an individual may wish to have a fully digital check-in experience at a hotel – including getting a digital key provisioned to their smartphone – but may be required by the hotel to first present their ID at the front desk before receiving a room key. We detail more of these use cases in Section VIII.

Questions for reviewers:
What should the threshold be for these use cases? Our intent is to focus on use cases that are not widely available in a fully online environment today for consumers because firms have a reason to ask for ID - not to create a loophole that will allow for VDCs to be used in any situation.

e. In both of the above categories of use cases, the fact that an online service provider has a legal, regulatory, or business requirement to collect identity data for one use case should not serve as license to collect identity data for every use case. And user consent for an online service provider to collect identity data for one use case should not be interpreted as having granted consent for every use case.

For example, while a bank has a legal and regulatory requirement to collect identity data for an individual seeking to open an account – and should be permitted to leverage VDCs to do so – that bank should not request identity data from an individual visiting its website to browse products or services. Nor should a hotel request identity data from an individual who is simply visiting its website to browse its rooms or facilities.

f. There are a number of potential use cases where online service providers have no legal or regulatory requirement to collect and validate data on an individual's identity, and where collecting identity information would not enable a service provider to make a product or service available online that would not otherwise be available. Use of a VDC for these purposes should be restricted.

For example, an online service provider should not collect identity information from a VDC to be used solely for marketing purposes, or as a tool to track consumer behavior online.

Question for reviewers:
Should wallets prohibit use of ID in these situations, or should there be options for individuals to still choose to share their data if they insist on doing so?

Could/should individuals be discouraged from sharing data with pop-ups and other warnings - but still be allowed to share if they choose to ignore them?

As noted earlier, the purpose of the Code is to create a tool that wallet providers and other stakeholders in the identity ecosystem can use as a way to prevent inappropriate requests for ID - however, we are trying to balance that with arguments that some are making that individual users should have the right to make their own decisions - even if they are "bad" ones.

We have also heard from some issuers that they are not comfortable imposing any restrictions on how individuals can use their VDC - raising questions about what sorts of limits wallet providers can impose on the use of a credential without some sort of tacit (if not explicit) approval from the credential's issuer.

This is one of the trickiest issues to resolve - we welcome ideas!

VIII. Use Cases and Associated Rules

In line with the five principles outlined above, the Code of Conduct defines three categories of use cases:

1. Use cases where online service providers have a legal or regulatory requirement to collect and validate data on an individual's identity – either a full credential, or sometimes a subset of attributes associated with that credential – and use of a VDC for these purposes should be explicitly permitted, provided that the request is for a subset of identity data directly relevant to the requirement.

2. Use cases where there is no legal or regulatory requirement to collect and validate data on an individual's identity, but in line with principle VII(c), organizations have historically required some proof of identity in person, or there is a strong risk and/or business case for use of a VDC.

   Question for reviewers:
   As noted earlier, we welcome input on what the threshold should be here.

   "Risk based" is probably too broad. "Business-critical risk" is tighter – but that may be too rigid?

   The intent here is to recognize that there are a number of things people do today where organizations generally require an ID to be presented - even though there is not a legal or regulatory requirement - and where the inability of someone to use their VDC to verify their identity (or something about themselves) online would preclude that use case from being available to people in a fully online setting.

3. Use cases that are restricted, given that there is no legal or regulatory requirement to collect and validate identity data, nor is there any significant risk-based justification or business case to collect VDC data.

In line with the Code's principles, here are the rules that apply to the following use cases in each of these categories:

1. Use cases tied to a legal or regulatory requirement

Note to reviewers: *The examples below are an early start on the use cases – there may be more in these verticals that we have not yet identified. Please let us know if there are others that should be considered for inclusion*

Financial Services *(largely taken from NIST NCCoE mDL Project)*		
Use Case	*Data Permitted to be Collected*	*Notes*
1. New account opening (CIP/KYC)	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	SSN is not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card) Attributes taken from https://pages.nist.gov/nccoe-mdl-project-static-website/nccoe-bank/assets/applying-for-an-account-CXjo9b1N.pdf
2. Setting up online access after an application is approved	Name DOB Address ID number Issuer of ID (i.e., what agency)	Attributes taken from https://pages.nist.gov/nccoe-mdl-project-static-website/nccoe-bank/assets/setting-up-online-access-ChMIgcqz.pdf
3. Instant approval (when CIP/KYC is fast tracked)	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	Attributes taken from https://pages.nist.gov/nccoe-mdl-project-static-website/nccoe-bank/assets/instant-approval-Dn7aO_9W.pdf
4. Preventing unauthorized high-risk transactions	Name Issuer of ID (i.e., what agency) ID Number	Attributes taken from https://pages.nist.gov/nccoe-mdl-project-static-website/nccoe-bank/assets/account_re-verification-BEwgUeVw.pdf
5. Account recovery (if a password or other authenticator is lost)	Name DOB Address SSN ID number	

	ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	

Health Care		
Use Case	*Data Permitted to be Collected*	*Notes*
1. Register for new patient portal	Name DOB Address SSN Issuer of ID (i.e., what agency)	SSN is not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card)
2. Telehealth ID verification	Name DOB Address SSN Issuer of ID (i.e., what agency)	See note above on SSN
3. E-Prescribe of controlled substances for health providers	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	See note above on SSN
4. Pick-up of prescriptions that are controlled substances	Name DOB Address ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency) Photo	Some states require confirmation that an ID be unexpired and include a photo and identification number (per https://www.cdc.gov/phlp/docs/menu-pdil.pdf)
5. Account recovery (if a password or other authenticator is lost)	Name DOB Address SSN Issuer of ID (i.e., what agency)	See note above on SSN

Government Services and Benefits		
Use Case	*Data Permitted to be Collected*	*Notes*

1. New account opening – applying for benefits	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	SSN is not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card)
2. New account opening – proving identity to set up an account at an e-government portal	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	See note above on SSN
3. Account recovery (if a password or other authenticator is lost)	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	See note above on SSN

Employment		
Use Case	*Data Permitted to be Collected*	*Notes*
1. New hire: Proving identity for I-9 compliance purposes	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	SSN is not available through a state mDL, but might be available through other VDCs yet to be created (i.e., a digital SSN card)
2. New hire: Background check associated with a new hire	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	See note above on SSN

3. Account recovery (if a password or other authenticator is lost).	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	See note above on SSN

Age-restricted products and services		
Use Case	*Data Permitted to be Collected*	*Notes*
1. Age Verification	DOB - or preferably, "Over a certain age" ID Expiration Date Photo (if needed for comparison)	Attribute requirements may vary across laws and regulations dealing with different age-related use cases; they also may vary state to state.

Vehicle Rental		
Use Case	*Data Permitted to be Collected*	*Notes*
1. Validation of ID and Driver's License at Pickup	Name DOB Address ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	

2. Use cases tied to a business or risk requirement

Note to reviewers:
The examples below are likely not an exhaustive list of use cases. We have identified for v1.0 of the Code those use cases which we believe are the most obvious candidates for use of VDCs in this second category, however, we expect this list may need to be broadened or revised in future iterations.

Hotels/Hospitality		
Use Case	*Data Permitted to be Collected*	*Notes*
1. Mobile Check-in without needing to visit the front desk	Name DOB Address Issuer of ID (i.e., what agency)	We welcome input from hotels as to what is actually needed

Education		
Use Case	*Data Permitted to be Collected*	*Notes*
1. Remote student enrollment	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	We welcome input from education stakeholders as to what is actually needed

Building Visitor Access		
Use Case	*Data Permitted to be Collected*	*Notes*
1. Mobile Check-in without needing to visit the front desk	Name ID Number	We welcome input from building security stakeholders as to what is actually needed

Ticketing		
Use Case	*Data Permitted to be Collected*	*Notes*

1. ID Verification for secure ticket transfers	Name DOB Address ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	We welcome input from ticketing stakeholders as to what is actually needed

Retail		
Use Case	*Data Permitted to be Collected*	*Notes*
1. Address validation for delivery	Name Address	We welcome input from retailers as to what is actually needed

Background Checks		
Use Case	*Data Permitted to be Collected*	*Notes*
1. ID Validation for background check associated with position of trust	Name DOB Address SSN ID number ID Date of Issuance ID Expiration Date Issuer of ID (i.e., what agency)	We welcome input from background check stakeholders as to what is actually needed

Account Recovery for Non-Regulated Use Cases		
Use Case	*Data Permitted to be Collected*	*Notes*
1. Account recovery (if a password or other authenticator is lost).	Name DOB Address	While VDCs should not be collected to set up accounts in the vast majority of non-regulated use cases, validated attributes from VDCs may be used by verifiers to match with data on file from customers as a “strong signal” to support account

		recovery for non-regulated use cases.

3. Use cases that are restricted

- Identity and/or Age verification to deliver targeted advertising
- Identity verification used similar to a cookie to track online behavior

Questions for reviewers:
Should the Code state that if a use case is not specifically called out above, it is restricted? Or should it be more open?

Are there other use cases the Code should specifically restrict here?

Can/should the code go as far as to formally prohibit a use case? Or is the decision to "prohibit" vs. "impose restrictions" one that should be left to the wallet provider or other credential manager?

As noted earlier, the purpose of the Code is to create a tool that wallet providers and other stakeholders in the identity ecosystem can use as a way to prevent inappropriate requests for ID - however, we are trying to balance that with arguments that some are making that individual users should have the right to make their own decisions - even if they are "bad" ones.

We have also heard from some issuers that they are not comfortable imposing any restrictions on how individuals can use their VDC - raising questions about what sorts of limits wallet providers can impose on the use of a credential without some sort of tacit (if not explicit) approval from the credential's issuer.

Appendix: Guidance and best practices for verifiers/relying parties

Verifiers making use of government-issued VDCs should use them responsibly. Below are some best practices that verifiers should abide by in their use of government VDCs.

- Data minimization - Verifiers shall collect only the minimum data necessary for a transaction.
- Purpose specification and transparency – Verifiers shall clearly explain to users what information is being requested, why it is needed, how it is being used, and how long it will be retained.
- Purpose limitation – Data collected for a transaction shall not be used for any other purpose outside of stated transaction, i.e., information from making a physician's appointment should not be sold to pharmaceutical companies.
- No sharing or selling – Verifiers shall not sell or share data from VDCs with any other organization, except as required by law.
- No tracking -- Verifiers shall not use VDCs to track individual behavior on their site or service, or across other sites or services.
- Right to Delete/Correct Data – Individuals should have the ability to delete or correct their data.
- Right to Alternative Path – Individuals shall not be forced to use a VDC to create an account and alternatives shall be made available, including in person or other options.
- No use of government-issued VDCs as an authenticator -- While government-issued VDCs will play a critical role in many identity applications, they are poorly suited for use as an authenticator. Verifiers should use passkeys or other authentication technologies, rather than link authentication to government-issued key material.

Questions for reviewers:
Are there other best practices or recommendations that should be included here?
Are there best practices we have listed that should not be included?