June 9, 2022

John Ohanian
Chief Data Officer
Director, Center for Data Insights and Innovation
California Health and Human Services Agency (CalHHS)

Re: Commentary on CalHHS Data Exchange Framework - Strategy for Digital Identities

Dear John:

Please find some thoughts I share coming from several decades of privacy and security expertise within the Banking and Payments industry. Tokenization is a proven technology to thwart Identity Theft. By design Tokenization is architected to manage a Secure Digital Identity. Tokenization is architected to secure Digital Identities in a complex ecosystem through the use of encryption, cryptograms and other digital device information along with rigorous Life Cycle Management. Tokenization removes sensitive personal information and stores it in a Remote Token Vault, which ensures actual personal data is NEVER exposed when data is at rest or on the move. Tokenization designed with these attributes achieves the Advisory Group's objectives for secure Digital Identities that ensure privacy and Identity Theft prevention. Tokenization ensures there is no replay value, meaning no way to retrieve sensitive personal data if Tokens are compromised in a breach. Tokenization of this type is built for speed and route-ability. Avivah Litan, VP & Distinguished Analyst at Gartner has noted tokenization has been used as an effective strategy for securing credit cards and it is a natural progression to use it to protect PII & EHR.

More recently, Sequent has been working on technology which addresses many of the gaps and weaknesses of digital identity in order to effectively shield sensitive clinical and financial information across the many stakeholders within the healthcare community.

We urge California Health and Human Services Agency (CalHHS) to consider adopting tokenization of unique identifiers within digital identities to reduce the threat of identity theft.

We recommend that CalHHS consider the following:

- Tokenization provides a single solution to meet the Digital Exchange Framework's need to establish, secure and provide consumer privacy, security and HIPAA compliance for BOTH Digital Identities and the statewide Person Index
- Tokenization is proven in the areas of privacy and security. Those two qualities, privacy and security, are essential to the successful implementation of the Data Exchange Framework

- Tokenization is architected to securely connect public and private entities like Healthcare Providers and Payors as well as government entities like Social Service agencies. Connecting the

participants in this ecosystem is imperative to achieving the goals of the Data Exchange Framework

- Tokenization is architected to enable consumers to access and control their Digital Identity and associated health and social service information from their mobile device privately and securely

In summary, Tokenization Systems are intended to enable secure and private communication among all the parties the Data Exchange Framework is addressing in the single Data Sharing Agreement and the common set of policies and procedures that govern and require the exchange of health information.

All my best,

Joan Ziegler
CEO