TESTIMONY OF SHAMSH HADI
CEO OF ZORROSIGN, INC.

BEFORE THE U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE & TRANSPORTATION

HEARING ON LEGISLATIVE PROPOSALS TO PROTECT CONSUMER DATA PRIVACY

DECEMBER 4, 2019

Chairman Wicker and Ranking Member Cantwell — thank you for affording me the opportunity to submit testimony to the committee as part of the committee's hearing to examine legislative proposals to protect consumer data privacy. My name is Shamsh Hadi and I am the CEO of ZorroSign, Inc. - a small company based in San Francisco, CA. ZorroSign is the pioneer of electronic signature technology and the developer of ZorroSign DTM, a unified platform, a complete Electronic Signature and Digital Transaction Management solution. ZorroSign's unique Document 4n6 (forensics) technology offers post-execution fraud detection and verification and authentication of electronic signatures and documents using blockchain tokenization.

I concur with members of the committee and the private sector that the United States urgently needs to pass a strong national data privacy law that will give confidence to all U.S. consumers that their data is safe and secure. As you know, Europe has taken the lead in this area with the implementation of the European Union's General Data Protection Regulation. It is incumbent upon the U.S. Congress to take up this issue and pass a comprehensive data privacy law.

Throughout my career in the high-tech industry, and especially through my work as CEO of a high-tech company that lives and breathes consumer data privacy and security, I have come to learn that blockchain can and should be an essential component to any consumer data privacy and security framework. In my testimony, I would like to share with the committee my views on how blockchain can and should be an essential feature of any national framework to safeguard consumer data and privacy.

According to a paper issued in February of 2019 by the National Institute of Standards and Technology (NIST Annual Manufacturing Series 300-6), *"blockchain is a distributed storage framework that is virtually tamper resistant, has a native synchronization-discrepancy-resistance mechanism and is already highly praised in the financial world."*

In its simplest form, blockchain is a shared fixed ledger for recording transactions. The concept of blockchain can and has been extended to have the highest levels of security and privacy protecting the sensitive information and identities of authorized individuals in a network who have permission to access the content stored in the ledger.

Blockchain is a digital record where all transactions are recorded in the order of occurrence and where the next record is linked and related to the previous record. It is a continuous database of records that can only be added to and never edited or deleted. In layman's terms, blockchain allows government agencies and businesses to secure and validate a digital asset, like a contract, enabling the enforcement of ownership or authenticity.

The noteworthy characteristics of a blockchain are:

- Indelible: The most important and distinctive property of blockchain. Once a transaction is written into a block, it can never be erased or modified by anyone, including the person who wrote the transaction.

- Globally Readable: Anyone who has permission to view the transaction can read what it contains and everyone sees exactly the same content.

- Accept Rules Based Rights: Any chosen party can write into the blockchain if it respects the predetermined rules set out for that transaction.

- Strictly Ordered: There is no ambiguity of the transaction. The audit trail will clearly show which block of data came first and which came second.

In its February 2019 paper, NIST noted that because blockchain *"…is tamper resistant and the blocks are timestamped, a blockchain is a robust solution to prove the existence of a specific asset at a certain time during the product lifecycle"* and "*a safe way to track both the existence and ownership of a digital asset at a certain time."*

There are a plethora of practical applications of blockchain in the real world:

- Banking: Financial transactions from opening an account to money transfers.

- Health care: Medical records and drugs composition.

- Real Estate: Track real estate transactions and tracking maintenance and upgrade of properties.

- Supply Chain Management: Tracking food supply from "farm to dining table."

- Contract management: Chain of Custody, Audit trail, and entitlement tracking.
- Retail: Protect consumers against issues of product authenticity. Using blockchain retail consumer goods can be tracked, eliminating the risk of consumers receiving counterfeit goods.
- Electronic Voting: Voter registration, personal identity, and voting records.
- Digital Identity: Securing and keeping track of your Personally Identifiable Information (PII).
- Diamond Industry: Using immutable tamper proof digital ledger, record: color, carat, certificate number (inscribed by laser on the crown or girdle of the stone), and origin in order to increase supply chain efficiency and eliminate conflict diamonds from market. Makes it possible to track diamond from origin to consumer.

Please note that blockchain is NOT Bitcoin. Cryptocurrency like Bitcoin uses blockchain, but they are not the same. Blockchain is not cryptocurrency or Bitcoin. Rather, Bitcoin uses blockchain to secure transactions and publicly record them in a distributed ledger.

Blockchain is important because it has unique qualities that set it apart from other transaction database management systems. Specifically, blockchain is being used today in private, permissions-based decentralized systems that are secure, trusted and automated with bank grade security. Ultimately, blockchain technology helps make digital transactions more secure, faster and less expensive.

One of the conclusions of the February 2019 NIST paper was that *"Due to its tampering resistance, blockchain is an ideal candidate to record and secure data exchanges."* As someone who has spent the better part of my career working on and with blockchain, I wholeheartedly agree with NIST's conclusion.

In terms of legislative proposals before the committee, I would respectfully suggest that any legislation setting national standards for consumer user privacy and data security require that any business or government entity that collects a consumer's Personal Identifiable Information (PII) have in place systems, products and services that ensure the privacy and security of that consumer's personal information and their data.

Such systems, products and services should prevent the unauthorized view/review, re-distribution and modification of personal information, and to the greatest degree possible:

1) Utilize Digital Security Certificates that never expire;

2) Employ blockchain tokenization technology to tamper-seal and verify actual users and authenticate documents and data, without the need for third-party authentication;

3) Ensure unbroken chain-of-custody of all consumer personal information and documents;

4) Provide a clear audit trail for every transaction that includes consumer personal information and/or documents;

5) Use a secure method of digital signatures if consumers are required to sign documents.

6) Employ authentication and user identity verification that does not rely on password-based log-in protocols, but instead employs biometrics or hardware tokens.

7) Replace password-based security verification with proof of identity via uniquely identifiable methods such as knowledge-based authentication, one-time password generator, Trusted device, hardware token, or the user's biometric signature (e.g. fingerprint, face, retina, etc.).

Any federal framework on data privacy that does not include the above requirements and recommendations would fall short of what is needed to fully protect consumer data and ensure the integrity of digital transactions — both in the public and private sectors. The thoughtful and intentional employment of blockchain to safeguard personal data is one way to achieve the dual goal of protecting consumers while at the same time preserving the economic and social benefits of data.

Thank you for your time and consideration. I would be happy to answer any questions committee members might have, either in person or in writing.