WRITTEN TESTIMONY OF
TODD WILKINSON
PRESIDENT AND CEO, ENTRUST DATACARD

HEARING ON
PROTECTING CONSUMERS IN THE ERA OF MAJOR DATA BREACHES

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

November 8, 2017

Chairman Thune, Ranking Member Nelson and members of the committee, thank you for the opportunity to discuss the recent major data breaches that have touched the vast majority of American consumers and the urgent actions necessary to protect sensitive personal information.

For almost 50 years, Entrust Datacard has provided solutions that enable the creation of secure physical and digital identities that are used around the world in banking, government and enterprise applications. Identity is a foundational element of our commerce system and the way Americans build their financial lives. The value of identity is the primary reason this information is targeted and why we continue to see more sophisticated attacks that lead to significant data breaches.

We live in an incredibly connected and complex world. The challenge of protecting data is an evolving and sophisticated task, but it all starts with a secure identity. This will only become more critical as we continue to drive toward greater connectivity, linking virtually every aspect of our lives to a connected system. According to the 2017 Verizon Data Breach Investigations Report, 43 percent of all data breaches can be traced to a phishing attack in which a malicious actor was able to compromise an identity and use this information to gain access to data. Once compromised, a primary target is consumer identities. The information stolen in the most recent breaches contained a significant amount of personally identifiable information (PII) belonging to millions of American consumers.

The focus of this hearing is to examine the recent data breach events, identify steps that could have been taken to better ensure the safety of consumer data and to determine if there are options to further safeguard consumer PII in the future.

Regarding the issue of steps that can be taken to better ensure the safety of consumer data, there are well documented best practices and numerous security tools available to mitigate common attacks. However, this committee can bring forward a number of experts, and most will agree that no system is free from vulnerabilities and all have the potential to be breached.

Additionally, a substantial amount of PII has already been stolen and can potentially be used to defraud consumers. It is essential to now find a balance between driving responsible behavior in enterprise security and providing an answer to the underlying security of the consumer identity. To address

consumer identity, it will be critical to implement a resilient identity system that can respond to compromise, with the ability to quickly recover and to ensure consumer data is no longer at risk.

The State of Identity Today

The implications of using an insecure identity go far beyond that of financial burden or inconvenience to the consumer. The use cases for our government issued identity stretch across all aspects of life, and if compromised, there is no process in place by which citizens can easily reestablish and recover their identity.

Commerce

Over the course of an eligible consumer's life they will engage in a variety of commerce activities that require the completion of an application that includes the public disclosure of their recognized identity – their social security number. From opening a banking account, to applying for a home or auto loan to requesting a new credit card from a big box retailer. While the application may take on a variety of forms — paper, digital and oral — the one thing each application has in common is that the citizen is put at risk of their personal identity credentials being compromised. Paper application documents that are not disposed of properly, or the breach of a digital database are common and easily compromise the consumer's identity. Yet, without the disclosure of the identity credential, a consumer is not be able to establish their identity and is restricted from conducting commerce.

Employment

The social security number was introduced in the 1930's as a means of recording and dispensing funds earned by citizens for retirement. The number was also intended for tax recording purposes.

When applying for employment, or when completing new employment paperwork, employees are required to provide employers with their social security number. Each time a person applies for a position and with each subsequent employment change, the applicant must provide an employer with their social security number.

Recent breaches of employee data have also been reported, exposing the personal information of millions. In June 2015, the Office of Personnel Management (OPM) announced that over 21 million records containing PII, including social security numbers, were stolen.

In the case of the OPM breach, the records compromised were tied to background investigation records, a common practice among many employers today. Many times, new employees are required to submit their identity for review by their employer. Should the identity of an individual be compromised without their prior knowledge, it could be career limiting: a background check of an employee whose identity has been compromised might falsely reveal financial difficulties or criminal histories – causing the applicant to lose the job opportunity and the employer to lose a valuable employee. The breach of personal information can also create the opportunity for bribery or blackmail from criminals or foreign powers that might hone in on those whose personal information reveals financial burdens or compromising information.

Insecure Identity: Risks and Impacts

To better illustrate this point, let's reflect on another major breach that occurred in 2013. In March 2014, one of my staff members at the time, David Wagner, testified in front of this committee in response to a breach of credit and debit card information by a major retailer that affected more than 40

million people. While this breach, and subsequent breaches of payment data, impacted consumers, they were able to quickly address the compromise. This is because the payment ecosystem was designed to be resilient. When fraud occurs, the liability largely falls to the financial institution not the consumer. In addition, financial cards are easily replaced by new payment credentials, thereby eliminating the risk of fraud on a compromised payment card.

The difference with today's conversation is that the compromised data is not a credit or debit card that can be easily replaced. It is a social security number, a name, an address that can have far reaching and long lasting impacts to those compromised. Over 145 million Americans' insecure identities are now forever at risk, and they have limited ability to protect themselves. A key question for this committee to consider is: What do we do now given these identities are forever compromised? The critical issue to address is the ability to recover from a data breach with a resilient secure identity.

Secure, Modern Identities

To address the challenges brought on by the current pattern of breached insecure identities, we should focus on how to help consumers recover. In today's environment, the only recourse a consumer has is to work with each credit reporting agency to lock their credit, ensuring that it cannot be used or to contract with a credit monitoring service that will do this on behalf of the consumer. The consumer is burdened with the cost and the time it takes to try to protect themselves.

Given most American consumer identities have already been compromised, it is imperative that action is taken to put the consumer back in control of how and when their identity is used. It is our strong recommendation that any use of personal information, whether an account opening, credit requests, transaction attempts, etc. require consumer authorization through a strong authentication mechanism. Putting the consumer in control could be implemented by leveraging the consumer's mobile device, as is common in banking applications today. The technology required for implementation is well tested and works at scale.

A modern secure identity system needs to strike a balance of providing an appropriate level of information to enable commerce activities, while providing consumers with the ability to quickly, and cost effectively, reestablish their identity and then move on with their lives without fear of further repercussions.

Key Characteristics of a Modern Secure Identity:

Identity Should Be Dynamic

As already mentioned, today's primary identity source, the social security number, is issued at birth and is difficult to change without significant inconvenience to the citizen. With a dynamic identity, a compromised identity can be revoked and replaced, reducing inconvenience or effort on the part of the citizen.

Dynamic identities are commonplace in Brazil, where Infraestrutura de Chaves Públicas (ICP) - Brasil issues digital certificates (a digital identity) for citizen identification. In this example, the government owns the core identity issuing technology, but partners with industry to provide consumer options for how to access this identity system. These certificates generally last one to three years and can be used to digitally sign documents with the same force as a written signature, access government systems online and provide easier and secure online access to financial institutions. A critical point is that ICP-Brasil has institutionalized the concept of dynamic identities. Even if the identity is not compromised, it

still has a relatively short validity period. And in the event of a compromise, the process to replace the identity with a new one is well understood and easily executed.

Identity is Easy to Issue, Revoke and Manage

We must be able to issue an identity (and revoke and re-issue it) without tremendous effort on the part of the user. When an identity is revoked, the revocation must be pervasive so that everyone can easily know what has been revoked and reissued. Payment cards are easily revoked; attempts to pay with a cancelled card are immediately declined.

The Consumer Controls their Identity

When individuals are personally accountable and in control of their own secure identities, they can determine which factors are in place to help confirm their identities. Identity factors are not reliant on data like address, telephone number, mother's maiden name or names of pets – these examples, like social security numbers, are static pieces of information that are easy for someone else to discover. Instead, more sophisticated factors like fingerprints and facial recognition could be used. Other factors, such as behavioral attributes and verifications through a mobile device, are also in wide use. The user can choose to confirm their identity through a variety of factors – a best practice in enterprise security is to use more than one factor. Individuals should have the ability to select which and how many factors to use, giving them control over how they secure and manage their identity.

A New Identity Framework

Our recommendation to this committee is that the time is upon us to create a new identity framework. This new framework would create a modern secure identity through a collaboration between government and industry. In all use cases, this new identity could minimize risk and inconvenience to the consumer in cases of breach, and allow a consumer to more easily recover their identity with minimal impact.

Our identity system today is broken - it is not secure. It is time to leverage available technologies to provide Americans with new mechanisms to protect their identities. In my company's previous testimony, we recommended the best path forward rests upon a private-public ecosystem that is built upon good security governance, secure identities and constant self-assessments of vulnerabilities. Whether we drive adoption via incentives or directives, we need to proceed now. I urge you to focus on near-term actions to address the consumer information that has already been compromised while working toward long-term solutions which create a more resilient identity.

Chairperson Thune, committee members, fellow panelists - Thank you for your time today.