United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

June 13, 2019

Dennis Gilmore
Chief Executive Officer
First American Financial Corporation
1 First American Way
Santa Ana, California 92707

Dear Mr. Gilmore:

On May 28, 2019, First American Financial Corporation (First American) reported that it had shut down access to one of its production environments that was found to have a design defect that created the potential for unauthorized access to customer data. It was separately previously reported on May 24, 2019 that the defect potentially exposed an estimated 885 million records related to mortgage transactions from as early as 2003 that included sensitive information, including bank account numbers, Social Security Numbers, driver's license numbers, and mortgage and tax records, without any required authentication.

Cybersecurity-related incidents have increased in frequency and potentially expose millions of Americans to fraud and theft that could have serious consequences for their financial lives. Bad actors are constantly looking to exploit any vulnerabilities for profit. It is essential that companies, particularly financial institutions, take the utmost care to maintain strong safeguards to protect any and all personally-identifiable information of U.S. consumers. As Chairman and Ranking Member of the Committee on Banking, Housing, and Urban Affairs, we are concerned about the scope and potential consequences of this cybersecurity-related incident, and seek additional information to better understand what happened and how First American plans to remediate all affected consumers for any loss or costs associated with the incident.

The report first identifying the design defect noted that these types of data exposures are some of the most common yet preventable. In an effort to better understand how individuals' data can be better protected and similar situations can be avoided in the future, please provide the Committee information to the following questions:

1) Regarding the timeline of events and responsible parties, please provide information on the following:

    a. The specific department and personnel responsible for maintaining the production environment in which the vulnerability was created, and internal processes for

monitoring production environments to identify and address any perceived vulnerabilities;

b. The dates and methods by which any department or personnel was first notified of the vulnerability and any subsequent actions taken regarding the vulnerability;
    i. Please explain the company's rationale if no initial immediate action was taken;
c. The specific date when senior management was first made aware of the vulnerability and subsequent actions taken by senior management;
d. The specific date when the Board of Directors was first made aware of the vulnerability, the dates of any Board meeting where the vulnerability was discussed, the names of the Board members participating in those meetings, and any subsequent actions taken or authorized by the Board; and
e. The specific date when law enforcement was notified of the vulnerability, and the processes and parties responsible for coordinating communication with law enforcement.

2) Please provide additional detailed information regarding the vulnerability, including:
    a. The nature of the production environment and vulnerability;
    b. How and when the vulnerability first originated;
    c. The amount of time for which documents were exposed;
    d. An estimate of the number of documents exposed and individuals affected;
    e. Whether there has been any unauthorized access to consumers' documents or information as a result of the vulnerability; and
    f. How the vulnerability went undetected through the company's normal cybersecurity assessments.

3) Please provide a complete list of all types of personally-identifiable information that was available without authentication through the production environment;

4) Please describe how First American secures Americans' personally-identifiable information, including whether it is compliant with PCI and NIST standards, is a member of the FS-ISAC, and identify the divisions of the company and employees responsible for ensuring the integrity and security of individuals' personally-identifiable information; and

5) First American has said that it plans to provide a mechanism for consumers who believe their confidential information has been compromised to report it to the company, and will provide credit monitoring services to affected consumers. Please describe any additional long-term plans to address the risks and any harms to consumers, including any resources set aside for future compensation and remediation for affected consumers.

We would appreciate your timely response to all of our questions.

Sincerely,

Mike Crapo
Chairman

Sherrod Brown
Ranking Member