ELIJAH E. CUMMINGS, MARYLAND
CHAIRMAN

ONE HUNDRED SIXTEENTH CONGRESS

JIM JORDAN, OHIO
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
http://oversight.house.gov

Opening Statement
Chairman Raja Krishnamoorthi
Hearing on "Improving Cybersecurity at Consumer Reporting Agencies"
Subcommittee on Economic and Consumer Policy
March 26, 2019

The Subcommittee on Economic and Consumer Policy is dedicated to addressing the issues affecting American consumers and our larger economy.

Today, we look at what can be done to improve data security by consumer reporting agencies, or CRAs.

September 7, 2017 changed our data security landscape forever. That was the day that Equifax announced that it had exposed the Social Security numbers and other sensitive information of nearly half of all Americans (148 million Americans to be exact).

That event educated many people for the first time about CRAs and the huge amounts of sensitive information they hold. What people still may not know is how many more of these companies exist. The Consumer Financial Protection Bureau, or CFPB, estimates that there are more than 400 CRAs in America.

Criminals want access to the treasure troves of data that CRAs hold. They want that information so they can open fraudulent accounts and run up debt in the names of innocent people.

In studying this issue, I was deeply saddened to learn about an Illinois resident whose credit was so badly damaged by identity theft, resulting from the Equifax breach, that the person was denied employment and housing. This is but one example illustrating the extreme and decades-lasting implications of allowing people's social security numbers, birth dates, addresses, driver's license numbers, and credit card information to be exposed to cyber criminals. And again, I want to let this sink in: this one particular breach has the potential to cause extreme harm to nearly half of the population, or 148 million Americans.

A year and a half has passed since the Equifax breach, and the causes of that breach have been investigated and exposed. Moving forward, it's our job in Congress to help prevent future data breaches, and to prevent more Americans from having their sensitive personal information compromised.

Through the Gramm-Leach-Bliley Act, Congress directed the Federal Trade Commission to implement data security rules for CRAs. To achieve that, it created the "Safeguards Rule," which requires CRAs to take "reasonable steps" to protect consumer data. But the FTC has

limited recourse against a CRA that violates the Safeguards Rule. It cannot seek penalties for first violations, and the FTC can only seek monetary compensation for consumers if they have identified a specific harm. Because the negative effects of a breach can often take years to surface, it is extremely difficult to reduce this harm to a dollar amount.

CRAs also hold huge sway over the lives of consumers – the information they control could determine if someone gets a loan, or a job, or insurance, or finds a home. Yet, CRAs are not accountable to those people. If consumers dislike a CRA, they cannot hold them accountable by taking their business elsewhere.

But Congress can hold CRAs accountable by giving federal watchdogs the tools they need to make CRAs care more about data security. Failure to implement proper data security must cost CRAs more than investing in good security to prevent a breach.

That is why today, Senator Warren and Chairman Cummings, released a proprietary report by the Government Accountability Office which we will closely examine in this hearing. In this new report, GAO has recommended giving the FTC penalty authority to prevent breaches and to protect data security. This is a nonpartisan analysis, and in fact, Democratic and Republican FTC Chairmen have called for increased penalty authority for first-time violations, including current FTC Chairman, Joseph Simons.

Enhancing FTC penalty power to enforce data security follows the model set by regulation in the banking industry. There, so far, we have avoided the type of large harmful data breaches that brought us here today.

Simply put, GAO does not think that the current regulatory system is strong enough to get CRAs to improve their data security. So far, CRAs have been able to internalize the profit off of consumer data, externalize the risk, and leave consumers holding the bag.

We also need to consider how consumers can protect themselves from the risk of identity theft. Last year Congress passed the Economic Growth, Regulatory Relief, and Consumer Protection Act, which requires CRAs to provide consumers security freezes. A security freeze locks down a consumer's credit so that fraudulent new accounts cannot be opened in their name. It is the best tool for preventing identity theft. We want to ensure that these consumer tools are actually accessible to consumers and are being utilized.

Today's hearing is the first step in ensuring the data of American consumers is being properly protected.

Contact: Aryele Bradford, Communications Director, (202) 226-5181