

Statement of National Consumer Law Center Staff Attorney Chi Chi Wu on the Equifax Data Breach that Affected 143 Million Consumers

FOR IMMEDIATE RELEASE: SEPTEMBER 8, 2017 || Contacts: Chi Chi Wu (cwu@nclc.org) or Jan Kruse (jkruse@nclc.org); 617.542.8010

The massive Equifax data breach is one of the largest in our country's history, affecting half of the United States population and nearly three-quarters of consumers with credit reports. Chances are, this affects YOU. Plus, the stolen information is the mother lode of sensitive personal data that can be used for identity theft: Social Security numbers, dates of birth, and in some cases, driver's license numbers. Also, was highly revealing credit reporting account information stolen, such as student loan or mortgage payment account numbers and payment histories? This information could be used for phishing schemes or other fraud.

Equifax should immediately pay or reimburse fees for security freezes to affected consumers at all three of the major credit bureaus, i.e. Experian and TransUnion in addition to Equifax. A security freeze is the most effective measure against "new account" identity theft, because it stops thieves from using the consumer's stolen information. Equifax is offering one year of its credit monitoring and identity theft prevention product in response to the security breach, which it states includes "the ability to lock and unlock Equifax credit reports." That is a first step, as the ability to lock Equifax reports is better than credit monitoring alone. Credit monitoring only informs consumers after the fact when there has been an attempt to open a fraudulent new account using the consumer's personal information. However, consumers need the ability to "lock down" or freeze their credit reports at all three major credit bureaus, and for more than one year, because the stolen information could still be used to fraudulently apply for credit using a report from Experian or TransUnion as well.

Equifax should immediately remove the forced arbitration clause and class action ban from the Terms of Use for its website and any credit monitoring or identity theft prevention services it offers. The arbitration clause does give consumers the ability to opt out of forced arbitration by notifying Equifax in writing within 30 days, which consumers should do. However, most consumers will not see that fine print and will be forced to give up their access to the courts. Through those terms, Equifax is purporting to prevent affected customers from access to the courts or the right to join together with the other hundreds of millions of injured consumers to jointly pursue claims against Equifax. A new rule by the Consumer Financial Protection Bureau would bar such forced arbitration clauses with class action bans, but members of Congress have threatened to block the rule.

Consumers affected by the breach should not wait to see if Equifax will pay for freezes at the other two credit bureaus; they should get freezes immediately if they are worried about identity theft. If consumers do not want to get a freeze, there is also the option of putting a 90-day "initial fraud alert" in their credit report that tells businesses they should verify your identity before they issue credit. The initial fraud alert must be renewed every 90 days.

Another risk of this massive data breach is tax identity theft, where crooks file phony tax returns in the consumers' name. The Internal Revenue Service (IRS) had previously made available Identify

Theft PINs for consumers in Florida, Georgia, and the District of Columbia, and consumers in those states should consider getting the pin (which they should do before getting a freeze). The IRS should make Identity Theft PINS available to all affected breach victims.

It's ironic that, on the same day that Equifax announced this data breach, Congress was considering a bill that would dramatically reduce the consequences of violating the Fair Credit Reporting Act (FCRA) for the credit bureaus and other industry players. H.R. 2359, the so-called FCRA Liability Harmonization Act, was discussed yesterday during a hearing by the House Financial Services Committee and would eliminate punitive damages plus limit class action damages under the FCRA. While the FCRA may or may not be directly implicated by the Equifax data breach, we need stronger, not weaker, consequences when companies violate long-standing privacy laws, such as the FCRA. Credit bureaus, such as Equifax, should not be rewarded with reductions in legal accountability given these recent events