Americans for Financial Reform
Center for Digital Democracy
Center for Economic Justice
ConnPIRG
Consumer Action
Consumer Assistance Council, Hyannis, MA
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Consumers Union
Electronic Privacy Information Center (EPIC)
Illinois PIRG
Massachusetts Consumers' Coalition
Maryland PIRG
MASSPIRG
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low-income clients)
National Consumers League
New Economy Project-NYC
PennPIRG
Privacy Rights Clearinghouse
Reinvestment Partners
U.S. PIRG
Virginia Citizens Consumer Council
VPIRG
WashPIRG
WISPIRG
Woodstock Institute
World Privacy Forum

8 October 2015

The Honorable Richard Cordray, Director, CFPB
The Honorable Edith Ramirez, Chairwoman, FTC

Via email

RE: Experian breach of T-Mobile customer and applicant data

Dear Director Cordray and Chairwoman Ramirez,

We, the undersigned organizations concerned with data privacy and consumer protection, write to express grave concerns raised by the early reports of the significant data security breach affecting T-Mobile customers and applicants whose information was stored by Experian. Experian has admitted that the data breach included "names, addresses, Social Security Numbers and birth dates, as well as other information from 15 million T-Mobile customers and

applicants." Experian admits that the breach affected customers and applicants who applied for T-Mobile services or credit during a two year period, from September 2013 through September 2015.

We believe that it is incumbent on the regulatory agencies to fully investigate this breach, including whether other Experian databases have been breached. As you know, Experian is one of the three nationwide consumer reporting agencies (CRAs), each holding data on over 200 million consumers. A data security breach that affected Experian's credit report files would be a terrifying and unmitigated disaster.

In one of its public statements about this data security breach, Experian made the following claims:

> "The server belonged to an Experian business completely separate from our credit bureau business. The incident did not impact our consumer credit database." (http://www.experian.com/securityupdate/index.html)

The information contained in what Experian calls a separate business appears to be header or identifying information, which is identical to the header or identifying information held in the Experian credit bureau database. This data could constitute a consumer report under the Fair Credit Reporting Act, as well as personal information protected by the Gramm-Leach-Bliley Act.

We have the following questions:

1) Was there a violation of the data safeguard rules under the Gramm-Leach-Bliley Act? What kind of data security standards is the CFPB requiring for the nationwide CRAs as part of its supervision of them as 'larger participants', and was there a violation of those standards?
2) What kinds of decision-making does this subsidiary provide? It appears to aggregate information used in credit transactions involving a consumer. How is its practice distinguishable from the sale of credit reports under the FCRA?
3) What kind of sharing of "header" or other credit information occurs across various Experian business platforms?
4) A separate Experian page (http://www.experian.com/marketing-services/partners.html) lists a variety of marketing partners. How does Experian firewall information contained in the credit report database differently from any information provided to these myriad partners?
5) What are the differences in security measures that would allow hackers to access the information of T-Mobile customers but not the main credit report files? If there are differences, why weren't the security measures used for the T-Mobile server? If there are no such differences, doesn't this raise the troubling possibility that the servers holding highly sensitive credit and personal information of over 200 million Americans is vulnerable to a data hack by identity thieves?
6) Is there any authority for the CFPB to require the nationwide CRAs to provide free security freezes to affected consumers? Are the CFPB and FTC willing to urge the nationwide CRAs to do so?

The undersigned organizations have worked on security breach issues for decades. We believe this breach, occurring at one of the nationwide CRAs, takes this problem to a whole new and dangerous level given the extraordinarily large amounts of critical financial information they hold. Identity thieves could play havoc of an unimaginably huge scale with access to such data, with potentially devastating consequences to consumers, financial institutions, and the American economy. We urge the CFPB and FTC to devote their fullest resources to addressing this issue.

If you or your staff have any questions, please contact Ed Mierzwinski of U.S. PIRG (202-461-3821 or edm@pirg.org or Chi Chi Wu at the National Consumer Law Center (617-542-8010 or cwu@nclc.org).

Sincerely,
Americans for Financial Reform
Center for Digital Democracy
Center for Economic Justice
ConnPIRG
Consumer Action
Consumer Assistance Council, Hyannis, MA
Consumer Federation of America
Consumer Federation of California
Consumer Watchdog
Consumers Union
Electronic Privacy Information Center (EPIC)
Illinois PIRG
Massachusetts Consumers' Coalition
Maryland PIRG
MASSPIRG
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low-income clients)
National Consumers League
New Economy Project-NYC
PennPIRG
Privacy Rights Clearinghouse
Reinvestment Partners
U.S. PIRG
Virginia Citizens Consumer Council
VPIRG
WashPIRG
WISPIRG
Woodstock Institute
World Privacy Forum

cc: FTC Commissioners Julie Brill, Terrell McSweeney and Maureen K. Ohlhausen
Jessica Rich, Director of the Bureau of Consumer Protection, FTC
Peggy Twohig, Assistant Director for Non-Bank Supervision, CFPB
Corey Stone, Assistant Director for Deposits, Cash, Collections and Reporting Markets, CFPB