ConsumersUnion®
POLICY & ACTION FROM CONSUMER REPORTS

September 14, 2017

Richard F. Smith
Chairman and Chief Executive Officer
Equifax, Inc.
1550 Peachtree Street, NE
Atlanta, GA 30309

Dear Mr. Smith:

Consumers Union, the policy and mobilization division of Consumer Reports,[1] is an expert, independent, nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. We write to express our deep concern about both the immediate and lasting effects of the devastating breach that was announced by Equifax on September 7, 2017.

Your company has estimated that the breach compromised the highly sensitive information—including social security numbers, driver's license numbers, and birthdates—of potentially 143 million consumers, nearly half of the U.S. population. The compromise of this information, apparently by malicious hackers determined to misuse it, leaves all affected consumers vulnerable to identity theft and other fraudulent uses of their information for years to come.

We recognize that Equifax, and likely many law enforcement agencies, are still investigating the facts surrounding the breach, as well as the question of whether Equifax had reasonable policies and protocols in place to protect the highly sensitive consumer data it collects, stores, and sells. However, it is clear that Equifax's response to date has been wholly inadequate. Your company has offered affected customers only one year of credit monitoring and, following public outcry, a limited and narrow opportunity to obtain a free credit freeze. The company provided inadequate and unreliable information about which consumers were victimized and what information was compromised, limiting consumers' ability to take steps to protect themselves. Equifax also originally forced victims visiting its site to waive their rights to

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of telecommunications reform, as well as financial services reform, food and product safety, health care reform, and other areas. Using its more than 50 labs, auto test center, and survey research center, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 7 million subscribers to its magazine, website, and other publications.

sue the company for the harms caused and, following public outcry, has not fully corrected this problem. Further, the company does not appear to have fully investigated—and certainly has not explained to the public—the sales of stock by three top executives just prior to public announcement of the breach.[2]

Given the extraordinary nature of this breach and the threat posed to nearly half of all Americans, Equifax has a responsibility to offer consumers the best resources and tools to help them protect themselves. We call on Equifax to take the following additional steps to help remediate the serious harm and ongoing risks to consumers:

1. **Pay for credit freezes.**

Security experts agree that the most effective remedy in the event of the exposure of sensitive data such as social security numbers is a credit freeze. By prohibiting others from accessing their credit records without permission, consumers can take control over their identity in the wake of a breach.

When it announced the breach, Equifax did not initially offer free credit freezes to affected consumers. Then, fully five days later, and only in response to massive public outcry, Equifax announced on September 12 that it was waiving Equifax credit freeze fees for the next 30 days. However, that window of time is still far too short, as consumers still have very little information about the extent of the breach. We urge Equifax to extend this waiver indefinitely and to clarify that (1) consumers who were previously charged will be automatically refunded and (2) Equifax will not charge consumers for subsequent actions to unfreeze and refreeze their records.

Moreover, consumers who wish to freeze their credit in response to Equifax's announced breach still must pay to freeze their records with other major credit bureaus in order to make the freeze effective. Many creditors, for example, consult only one credit bureau for a loan applicant. The sensitive personal information compromised in the breach can thus be used to fraudulently obtain credit and cause other harm without Equifax being contacted. We urge Equifax to pay any fees associated with credit freezes at other credit bureaus so that consumers can prevent their data from being improperly used in connection with other credit bureau records.

2. **Extend credit monitoring for affected consumers.**

[2] Other missteps that should and could have been avoided include: 1) the PIN generated for an Equifax credit freeze should not have been a timestamp of when the consumer requested it 2) consumers should not have been asked for credit card information in order to sign up for free credit monitoring, and 3) Equifax hosted information about the breach on www.equifaxsecurity2017.com, an irregular and easily spoofed domain.

To date, Equifax has offered one year of free credit monitoring to consumers possibly affected by the breach. Credit monitoring provides less protection than a credit freeze, but does provide useful and immediate information that could be used to limit the consequences of identity theft after the fact. However, the risks to consumers due to this breach are not limited to one year—data exposed to hackers could be used to open fraudulent accounts several years in the future. For this reason, Equifax should extend credit monitoring indefinitely for all consumers potentially affected by the breach. If Equifax subsequently determines that there is a reasonable likelihood that sensitive data such as a social security number has been breached for certain consumers, Equifax should extend its credit monitoring for those consumers for life.

3. **Provide more detailed information about the security incident.**

While Equifax has been aware of the security incident since July, it has to date provided only very vague information about the breach and about what consumer data was compromised. The initial Equifax statement confusingly stated that while the breach "potentially impact[s] 143 million consumers," the company's core consumer and commercial credit databases were unaffected. Providing more information about *which* databases were compromised could help consumers and regulators determine how best to respond.

Moreover, while consumers have been told that the compromised databases *include* information such as social security numbers, email addresses, financial account information, and birth dates, there is no way for consumers to determine what particular data elements were exposed about each of them individually. Equifax has provided a tool for consumers to see if they were compromised, but that tool only indicates "we believe that your personal information may have been impacted by the incident," with no indication of what information was or was likely exposed. Further, consumers have reported inconsistencies in the tool, such as providing different responses for the same personal information submitted through different devices, or indicating likelihood of compromise for invented and implausible names.

To prevent further harm to consumers seeking to protect themselves, Equifax must upgrade its tool to provide more detailed information about precisely what types of data were breached for each affected consumer. Knowing what data was exposed can guide consumers in choosing which steps, in addition to security freezes and credit monitoring, they must take to avert additional forms of identity theft, such as medical or tax fraud. If this tool cannot be fixed or replaced, it should be taken offline immediately, so that consumers do not rely on inaccurate information to their detriment.

Finally, while we understand that the causes of the breach are still under investigation, we call on Equifax to commit to a full public explanation and accounting of the compromise, and what security measures and procedures were in place to protect consumer data. Given the

sensitivity of the data that Equifax holds, the importance of this data in granting or denying important consumer benefits, and the fact that consumers have little or no control over either, Equifax has a heightened responsibility to be fully transparent about what has happened, in order to minimize the damage and forestall similar episodes going forward.

4. **Remove all mandatory arbitration clauses.**

When Equifax announced the breach, its terms of use for the credit monitoring tool stated in fine print that consumers were waiving their rights to sue and instead would submit to mandatory arbitration. Imposing this condition on victims of the breach was met with strong public criticism, and for good reason—forced arbitration deprives consumers of access to public courts of law, undercutting fundamental legal protections.

Equifax has repeatedly changed its story about whether and how the mandatory arbitration clause impacts consumers. Following public outcry when consumers and the media noticed the clause, Equifax announced that it would apply only to the special new credit monitoring service, and not to the breach itself. Even then, another arbitration clause remained in effect for other consumers who signed up for its existing credit monitoring service. Further, all consumers who interact in any way with the site remained subject to yet *another*—and far broader—binding arbitration provision purporting to cover "any claim, dispute, or controversy between You and Us relating in any way to Your relationship with Equifax." Equifax is now saying that none of these clauses will apply to consumers harmed by the data breach *or* who sign up for credit monitoring services. However, the clauses have not been removed and could be changed at any time, so it is still unclear whether or how they could still be used to prevent consumers from having their day in court.

Equifax does a huge disservice to consumers by including mandatory arbitration clauses in boilerplate legal terms forced on consumers. While the information that Equifax collects, stores, and sells play a vital role in the U.S. economy, consumers do not generally make a choice about providing it, and have little opportunity to hold Equifax and the other credit bureaus accountable. Equifax should not try to insulate itself from accountability even further by forcing consumers into private, company-selected panels that operate in secret and are not bound by law or legal precedent.

5. **Commit to hiring and training sufficient staff to review and process disputes promptly.**

Given the enormity of the exposure, Equifax needs to be prepared for a deluge of problems, and must have sufficient resources on hand to resolve these problems quickly and

effectively. The company should not wait for these problems to pile up and then address a mounting backlog. In addition to hiring more call support staff to address consumer inquiries, Equifax should act now to hire and train the staff needed to keep any backlog from occurring. Equifax should also commit to resolve disputes promptly, consistent with the requirements under federal law.[3]

6. Set aside a fund to compensate consumers whose data has been exposed.

As Equifax investigates the full extent of this breach, it will gain a better sense of the potential long-term risks to consumers for identity, tax, and medical fraud. Equifax has an obligation to American consumers to compensate them for the injury they may incur for years to come. Accordingly, Equifax should create a substantial and dedicated reserve account to compensate consumers affected by this breach.

7. Investigate allegations of insider trading and hold wrongdoers accountable.

Finally, we have followed news reports that three senior Equifax executives sold a significant amount of Equifax stock after the internal discovery of the data breach on July 29, but before it became known to the public or to regulators. The timing of these sales—a handful of days after the initial uncovering of a massive security incident—raises major red flags. However, Equifax's initial reaction was disappointing and troubling: first, its press statement sought to minimize the scope of $2 million in sales as "small." Second, rather than stating an intention to investigate the issue, Equifax casually and summarily dismissed the allegation of trading on nonpublic information with no apparent inquiry at all—much less a rigorous one. It seems surprising that the Chief Financial Officer of the company would not have been notified in advance of the massive liability exposure the breach posed for the company. Equifax should immediately act to preserve all documents and communications of the executives in question, and commit to an independent investigation of the possibility of insider trading.

[3] The Fair Credit Reporting Act generally requires that disputes be resolved within 30 days. 15 U.S.C. § 1681i(a)(1)(A).

Conclusion

Although we understand that Equifax is adapting in real time to a fast-moving situation, the consumers injured by this breach should be the company's first and foremost priority, and Equifax should commit to their protection and to making them whole. There is much more that could and should be done in light of the significant risks to consumers caused by this enormous breach. We urge Equifax to address the many concerns discussed above, and to continue to look for new ways to protect consumers from the potentially catastrophic harm this breach could cause.

Sincerely,

Jessica Rich
Vice President, Policy and Mobilization

Justin Brookman, Director, Consumer Privacy and Technology Policy

Consumers Union
1101 17th Street, NW
Suite 500
Washington, DC 20036