taproot® security

Rep. Jeb Hensarling, Chairman
Rep. Maxine Waters, Ranking Member
Financial Services Committee
2129 Rayburn HOB
Washington, DC 20515

Sen. Mike Crapo, Chairman
Sen. Sherrod Brown, Ranking Member
Banking, Housing, & Urban Affairs Committee
534 Dirksen SOB
Washington, DC 20510

September 29, 2017

Dear Committee Members,

The Equifax security breach brought to light consumer protection issues unforeseen by the Fair Credit Reporting Act, and therefore never addressed in FCRA legislation or CFPB rule making.

The closest FCRA comes to addressing this scenario is the *Summary of Rights of Identity Theft Victims* provision[1] directing CFPB to provide a "summary of the rights of consumers under this title with respect to the procedures for remedying the effects of fraud or identity theft". A "victim" is defined as a "consumer whose means of identification or financial information has been used or transferred … without the authority of that consumer, with the intent to commit … an identity theft or a similar crime."

Since a credit agency security breach involves unauthorized disclosure of protected consumer data for the purpose of fraud or identity theft, it fits precisely within the definition above. However, the *Summary of Rights* CFPB created under FCRA does not adequately address a large-scale breach. The Bureau's *Remedying the Effects of Identify Theft* publication offers victims access to free fraud alerts, two free credit reports, and the right to challenge fraudulent transactions or related debt collections.

Such remedies may suffice in a garden variety identity theft case, but are proving inadequate after a massive cyber breach. In the event of such a data loss, credit agencies should take additional steps:

1. proactively notify victims when possible (not wait for them to submit inquiries);
2. never ask victims to accept binding arbitration in lieu of other legal remedies;
3. waive fees for credit freeze or security freeze requests;
4. waive fees for PIN or password changes;
5. share technical details of the incident with CFPB and other applicable federal authorities;
6. accept fines or civil penalties imposed by CFPB

We urge the Committee to modernize FCRA, giving consumers these additional protections in the event of credit agency security breaches, and directing CFPB to revise its rules accordingly[2].

Taproot Security is a private firm advising clients and policymakers on vital cybersecurity matters, with particular emphasis on the US financial services sector.

[1] § 609 - 15 U.S.C. § 1681g(d)
[2] CFPB has announced its intent to revise FCRA rules in RIN 3170-AA54

Thank you for this opportunity to share our perspective on FCRA and cyber security.

Sincerely,

Michael McCormick
President, Taproot Security
www.taprootsecurity.com
mike@taprootsecurity.com