After Breaches, Acts of Contrition

Adam Shostack and Andrew Sudbury

Submitting author: Adam Shostack, ,

Abstract: The "acts of contrition" companies take after breaches do not reflect consumer privacy preferences, and are at odds with such preferences. We will present two surveys showing such preferences. We suggest a practical solution.

Background: For FTC PrivCon 16, the one author submitted a proposal "The Breach Response Market Is Broken."[1] The essential insight of that short paper is that companies buy breach response services "on behalf of" consumers, but do not take their preferences into account. Having seen that submission, Andrew Sudbury and colleagues ran a survey which confirmed some of those hypotheses.[2] Since that submission, the Equifax breach happened and attracted a great deal of attention.

That attention has included no fewer than 240 lawsuits, SEC and FTC investigations[3] and an investigation by the House Energy and Commerce Committee.

Despite this white-hot attention, Equifax showed failures of execution in their offer to customers. They offered a credit monitoring product for one year. The offer was rife with sign-up failures.[4] Their tool to allow citizens and residents to check if they were impacted always gave the same message about "you may have been affected" regardless of what data was entered into its tool.[5] Equifax even sent links to a phishing site to those who engaged with

---

[1] https://www.ftc.gov/system/files/documents/public_comments/2016/10/00035-129137.pdf

[2] https://www.abine.com/blog/2016/extremely-limited-innovation-in-protecting-consumers-from-data-breaches/

[3] "Equifax faces hundreds of class-action lawsuits and an SEC subpoena over the way it handled its data breach," Hayley Tsukayama, The Washington Post, November 9, 2017 https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach/

[4] "Equifax has offered free credit monitoring after its epic data breach. Here's what happened when some people tried to sign up." Michelle Singletary, The Washington Post, September 21, 2017 https://www.washingtonpost.com/news/get-there/wp/2017/09/21/equifax-has-offered-free-credit-monitoring-after-its-epic-data-breach-heres-what-happened-when-some-people-tried-to-sign-up/

[5] Equifax offered a tool that allowed people to check if they were amongst those whose data had been exposed. It worked by asking for a last name and 6 digits of an SSN. It provided the same response even when people entered random data. Such random data should not have matched any record or file in Equifax's system. So the issuance of the same response may indicate either deception or incompetence on the part of Equifax. "PSA: no matter what, Equifax may tell you you've been impacted by the hack", Sarah Buhr, TechCruch, September 8, 2017. https://techcrunch.com/2017/09/08/psa-no-matter-what-you-write-equifax-may-tell-you-youve-been-impacted-by-the-hack/

them on Twitter,[6] and even after they were alerted to the problem, continued sending the phishing links for *nearly two weeks.*[7]

Lastly, Equifax has offered it's own "TrustedID Premier" service as its "act of contrition."

It is our belief that consumers probably do not think that's a fair offer or a meaningful act of contrition. They might prefer a product offered by someone who displays better execution, or even choice in the selection of fixes. We are currently running a survey to test that belief.

We suggest that the FTC use Equifax as an opportunity to explore new and innovative responses within consent decrees, including requiring that Equifax issue vouchers to impacted individuals, so that those vouchers can be used by victims to select a service to help them deal with the problems that Equifax has caused. Vouchers would let people better exercise additional control over their personal information, and address a potential market issue where everyone having access to a free and low quality identity protection service might be market-distorting.

The new research we will present is the results of the two surveys, one completed and published, and one in progress.

Note: both authors are writing as individuals, not as representatives of any organization.

[6] "Equifax tweets fake phishing site to concerned customers" Selena Larson, CNN, September 20, 2017

[7] "Equifax Has Been Sending Consumers to a Fake Phishing Site for Almost Two Weeks" Dell Cameron, Gizmodo, September 20, 2017, https://gizmodo.com/equifax-has-been-sending-consumers-to-a-fake-phishing-s-1818588764