Title: The Breach Response Market Is Broken (and what could be done).
Adam Shostack,

Abstract: Nearly ten years ago, Andrew Stewart and I predicted the creation of a robust market for helping people after breaches [Newschool]. That market has not emerged. My own experience in 2015 made me reflect on the source of the market failure. This talk details the problem and offers up a possible solution.

Findings:

(1) In 2016, credit monitoring is the default olive branch companies and government agencies extend after a breach.

(2) In 2016, breaches are frequent enough that most Americans have credit monitoring available to them as a breach remedy. [Bitglass, Gemalto]

(3) Credit monitoring is offered in a wide range of circumstances. In many of those circumstances, it is of limited value. For example, credit monitoring is offered to breaches of credit card theft, where the risk of new account fraud is low. It is offered in breaches of medical data, where credit monitoring may help with financial risk, but does little to address the risk of intermingled medical records, or the privacy issue of having medical history leaked. Experts express skepticism over the value of such services, and bemoan their many failings. [Krebs, Burke]

(4) Post-breach credit monitoring is marketed and sold to companies who have leaked information, not to the individual whose information was leaked.

(5) Post-breach credit monitoring is not consumer-friendly. For example, I have two concurrent accounts with the same company. There is no difference I can discern, but the company was unwilling to combine them to run one after the other, as “they were billed to different organizations.” Their customer service is awful, and I would never voluntarily give them a dollar.[1]

(6) Consumer behavior shows skepticism about today’s market offerings. Only 3-5% of victims sign up for credit monitoring after large breaches. [Katz] Companies may have an incentive to make signup difficult, as they pay for each signed-up victim. Recent research by RAND disputes these numbers, and refers to the discrepancy between their result and previous results as “startling.” They also say “Furthermore, of participants who reported not having accepted offers, many cited their reason as already having such a service.” [Ablon]

(7) Few or no new services are emerging to address these gaps. Despite consumer skepticism, the availability of free substitutes creates challenges for new market offerings. Any new entrant has to offer enough extra value to convince consumers to buy a service. This challenge is amplified because investors are wary of funding new entrants to a distorted market.

[1] For example, I get two emails, minutes apart, telling me I need to login to each account. If I login to just one, they nag me about logging into the other to “view important information.” The provider knows the two accounts are tied to the same SSN, they know I’ve viewed it.

Proposal:

a) The FTC should use its consent decree process to ensure that citizens and consumers are well served after a breach. Companies submitting to a consent decree should be required to provide a voucher to people whose information has been leaked. This would allow people to buy services that they want, rather than the service that a company selects for them. Consumers could make choices about service levels, length of service, appropriateness of a service to the threat, or other factors. (It would be reasonable for the company, in conjunction with the FTC, to make a recommendation.) Over time, the existence of vouchers would likely become a new, more citizen-centric and market friendly olive branch.

b) The FTC should study the rate of adoption of credit monitoring, the satisfaction of citizens with credit monitoring, and related factors to better inform policymakers about possible market failures.

Disclosure: The author is a shareholder in AllClear ID, who provides breach-related services. The proposal is a result of a frustrating experience with credit monitoring, as related in section 5, and will be shared with AllClear ID.

References

(All references accessed September 2016)

[Ablon] Ablon, Lillian, Paul Heaton, Diana Lavery and Sasha Romanosky. “Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information.” Santa Monica, CA: RAND Corporation, 2016. http://www.rand.org/pubs/research_reports/RR1187.html.

[Bitglass] “One in Three Americans Affected by Healthcare Breaches,” press release Jan 27, 2016 at http://www.bitglass.com/press-releases/bitglass-report-one-in-three-americans-affected-by-healthcare-breaches-in-2015

[Burke] “‘Free credit monitoring’ after data breaches is more sucker than succor,” Kathleen Burke, Marketwatch, June 10, 2015, http://www.marketwatch.com/story/free-credit-monitoring-after-data-breaches-is-more-sucker-than-succor-2015-06-10

[Gemalto] “Data breach statistics 2016: First half results are in,” Andrew Gertz, Gemalto Blogs, September 20, 2016 http://blog.gemalto.com/security/2016/09/20/data-breach-statistics-2016-first-half-results/

[Katz] “Way More Feds Signed Up for Post-Hack Protections Than Anyone Anticipated” Eric Katz, Government Executive, July 28, 2015t http://www.govexec.com/pay-benefits/2015/07/way-more-feds-signed-up-for-post-hack-protections-than-anyone-anticipated/118668/, accessed September, 2016.

[Krebs] “Are Credit Monitoring Services Worth It?” Brian Krebs, Krebs on Security, March, 2014 https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ accessed September, 2016.

[Newschool] *The New School of Information Security,* Adam Shostack and Andrew Stewart (Addison-Wesley, 2008)