Forgive and Forget?: What happened after the Equifax and Uber data breaches

Kristen Moran

December 14, 2019

Abstract

Every day we willingly submit our personal information to more and more digital databases, from credit cards and emails for our Netflix subscriptions to social security numbers and birth dates for bank accounts. We provide all this important personally-identifying information with somewhat blind trust in the companies. So what happens when that trust is betrayed, when hackers/crackers break their way in and get a hold of all this sensitive information? News articles are written, the media coverage lasts a cycle or two, but then the story mostly fades away. But what happens to all that breached data? For the estimated 83% of people who reuse the same or similar passwords across sites, do passwords get changed? Do affected users even get directly notified? And are the consequences clearly explained or understood? Do the companies face consequences themselves? This paper will take a look at two of the most grossly mishandled data breaches in recent history and analyze the aftermath, long after the news cycles forgot about them.

1 Introduction

We increasingly live in a digital world. Debate rages on about if data is "the new oil", but whether it is officially the most valuable resource or not, its power is undeniable. As Cambridge Analytica showed the world in 2016, there is power in data — enough power to win an election and manipulate people on an individualized basis.

So how do we handle protect our data in a world where we so freely give it to others? This essay aims to find an answer to that question by examining moments where data is at its most vulnerable – major data breaches – and seeing what these companies take care of, and what they leave for us to do ourselves.

2 To the Community

Digital data is also omnipresent — it is quite literally everywhere we go, following us on our phones, on our watches, and in our wallets, with each credit card swipe. Our locations, our spending habits, our exercise routines are collected like breadcrumbs that we drop as we go about our lives. Sometimes we leave a whole loaf of bread — when we voluntarily give up large swaths of personal data like our emails, our addresses, our phone numbers, even going to the most sensitive types of information — social security numbers, bank account details, and passwords to our accounts. I have all my passwords saved under my Google account — if there's ever a data breach there, everything I have ever done online will suddenly be vulnerable.

I am as much a product of this age as everyone else. I was driven to write this paper over personal concern — what happens to my data after a security breach? If I am to argue that educating oneself is the best defense, writing this paper was my own first step down that path.

3 Background

So just how have data breaches been handled? Looking at just the past decade, the decade in which the public and companies have been most informed of the sensitivity with which data must be handled, many notable data breaches have taken place.

It's pretty difficult to find information on the exact response on the companies' ends to data breaches — security improvements are rightfully kept fairly private, so as not to

provide crackers any helpful information. But the more recent data breaches have been more critically received, so their public response has been more closely documented.

Equifax The example that comes to mind is the Equifax breach of 2017. After discovering that 143 million consumers' data was breached, the company took a month of internal investigation before publicly announcing the breach — strike one.[1] As the company investigated, compromised users were at-risk of further exploitation — and they didn't even know it.

After making the breach public, Equifax set up a website to allow users to check for themselves if their data had been involved: equifaxsecurity2017.com. While a good idea in theory, in practice it was less than satisfactory as "lookalike domains are often used by phishing scams, so asking customers to trust this one was a monumental failure in infosec procedure".[2] The website also, for a time, incorrectly told everyone who checked that they had been affected by the breach, even if they had not. And the social media outreach directed some 200,000 users to the wrong website. Strike two.

Equifax was back in the news recently, as the FTC settlement was reached this summer. A cash payout was made available to all those impacted, up to $125, out of a total $31 million.[3] The problem, however, is that $125 expects only 248,000 people to file a claim — .17% of those affected. This illustrates that Equifax anticipated only a tiny percentage of victims to care enough, know enough, and pay enough attention to follow through — an insult to the people whose trust they have already lost. Strike three.

Uber Another recent example of what not to do is Uber. In late 2016, 57 million riders and 600,000 drivers had their Uber accounts compromised. Names, email addresses, and phone numbers of riders, and drivers license numbers of drivers were accessed.[4] However, Uber sat on this information for a year before telling its users, after they believed they had handled the situation.

The handling, however, was an entirely new set of problems in itself. The crackers who broke in were paid $100,000 — essentially rewarded for their illegal activity under the guise of a bug bounty. It came with the stipulation that the stolen data be destroyed, but Uber had no way to verify that this actually occurred. Uber also fired their Chief Security Officer

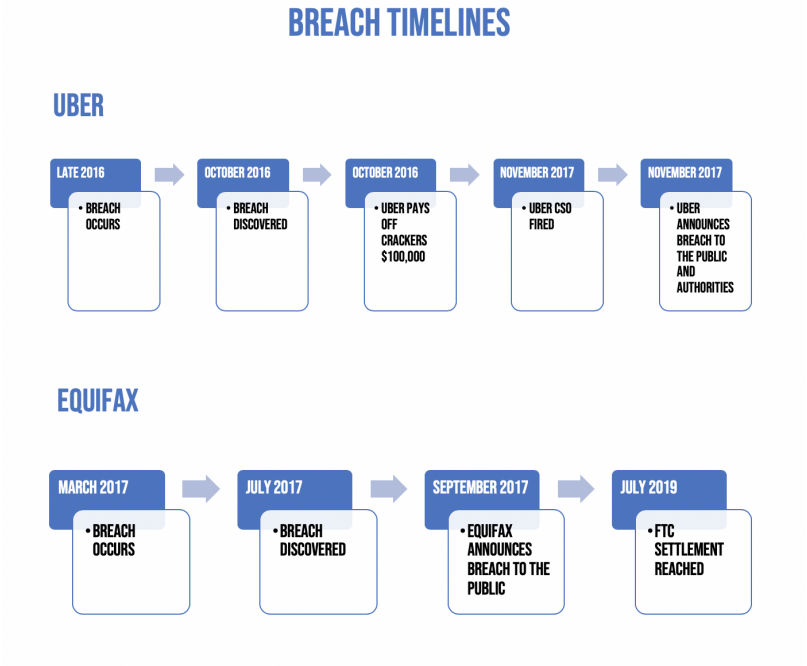
[1] https://www.secureworldexpo.com/industry-news/day-by-day-timeline-of-equifax-breach

[2] https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

[3] https://fortune.com/2019/07/31/equifax-data-breach-settlement-funds

[4] https://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html

— a bad public appearance to blame one of their own, instead of the crackers.[5] Uber's valuation dropped $20 billion – inarguably in part due to the breach.[6] Uber also lost $148 million directly due to the breach through its settlement.[7]



Summary of Responses While neither Uber nor Equifax had passwords stolen as part of their breaches, the valuable data stolen still needs to be protected. While it isn't possible to just update a Social Security Number, there are steps these companies can take – and did, to an extent. The table below outlines these responses, as well as the financial consequences each company faced:

	Did stolen information get changed/protected?		Notified impacted users directly?		Company consequences	What happened to the data?
Equifax	1 year of opt-in free credit monitoring		*those with concrete financial loss*	*other impacted users*	$45 million *in financial loss claims* $31 million *in other claims* $700 million *FTC settlement*	unknown
			yes	no - all users told to check website		
Uber	*drivers*	*riders*	*drivers*	*riders*	$148 million *FTC settlement* $20 billion *valuation drop*	deleted
	free credit monitoring and identity theft protection service	monitoring the affected accounts	yes	no		

[5] https://www.nytimes.com/2017/11/21/technology/uber-hack.html?action=click&module=RelatedCoverage&pgtype=A

[6] https://www.thestreet.com/markets/mergers-and-acquisitions/uber-s-rough-road-leads-to-softbank-deal-14431727

[7] https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html

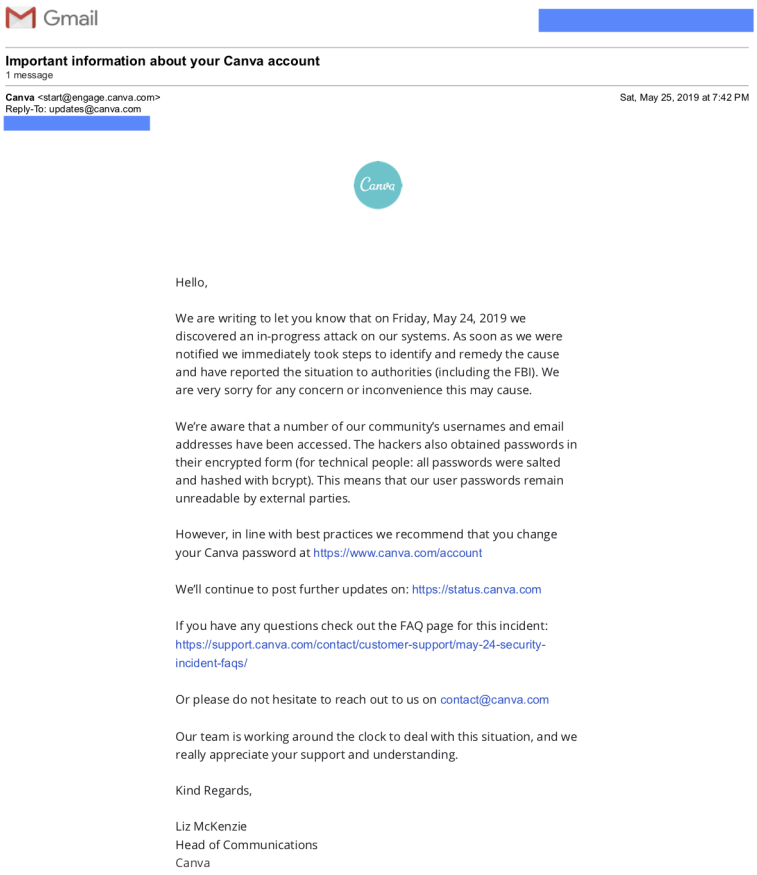
Important to note: while Uber did eventually directly notify its impacted drivers, it took them a full year to do so.[8] Also, Equifax's response to protecting the credit of those impacted looks good on paper, the fact that the services are opt-in means only users who know they were breached can take advantage of the offer. And because Equifax did not notify users directly, this number is shockingly low. Only 26% of Americans checked their credit reports within two weeks of the breach – an estimated 61 million people.[9] This leaves a lot of impacted users unaware and vulnerable.

4 Action Items

So what do you need to know? As a consumer who trusts these large institutions with personal data, stay aware. Think critically about what data you give away, and to whom. Obviously, you have to share some personal information with some companies, but don't do so blindly. Listen to the news, and pay attention to any communications regarding sensitive accounts you may have. Even for the not-so-sensitive accounts, make sure to read those "Login Attempted" emails — stealing a password from somesillywebsite.com is much easier than Bank of America, but odds are you use some form of the same password for both.[10]

Any awareness is an advantage. While writing this essay, I looked up my own email on haveibeenpwned.com — imagine my surprise at finding that my data had, indeed, been breached! The graphic design website canva.com was breached in May of this year, and stolen data included emails, usernames, and (encrypted) passwords. Searching my email did turn up an email from Canva, shown below:

[8] https://us.norton.com/internetsecurity-emerging-threats-uber-breach-57-million.html
[9] https://www.lifelock.com/learn-data-breaches-equifax-data-breach-2017.html
[10] https://www.cyclonis.com/report-83-percent-users-surveyed-use-same-password-multiple-sites/



Gmail

Important information about your Canva account
1 message

Canva <start@engage.canva.com>
Reply-To: updates@canva.com

Sat, May 25, 2019 at 7:42 PM

Hello,

We are writing to let you know that on Friday, May 24, 2019 we discovered an in-progress attack on our systems. As soon as we were notified we immediately took steps to identify and remedy the cause and have reported the situation to authorities (including the FBI). We are very sorry for any concern or inconvenience this may cause.

We're aware that a number of our community's usernames and email addresses have been accessed. The hackers also obtained passwords in their encrypted form (for technical people: all passwords were salted and hashed with bcrypt). This means that our user passwords remain unreadable by external parties.

However, in line with best practices we recommend that you change your Canva password at https://www.canva.com/account

We'll continue to post further updates on: https://status.canva.com

If you have any questions check out the FAQ page for this incident: https://support.canva.com/contact/customer-support/may-24-security-incident-faqs/

Or please do not hesitate to reach out to us on contact@canva.com

Our team is working around the clock to deal with this situation, and we really appreciate your support and understanding.

Kind Regards,

Liz McKenzie
Head of Communications
Canva

But as the average user received 121 emails per day in 2015[11] — undoubtedly greater by now — I understandably never read this email. There's a chance I never saw it at all, and a chance I saw the subject line but didn't think there was anything that important about my Canva account. Now I know better.

I'm not alone in my original response to the breach. A study done found that users who were presented with breach warnings opted to entirely ignore 25.7% of them – almost equal to the 26% of warnings that actually caused users to create new passwords.[12]

And as a company — wise up. Security is a field that requires action, not reaction. Invest in your defense before you've lost the data of your customers — and their trust. Any cost of proactive security will be greatly outweighed by the money not spent on recovery efforts, and not lost due to dropping in public opinion. The world is moving fast, and crackers are moving with it. Keep up.

[11] https://www.cityam.com/inbox-anxiety-how-regain-control-email

[12] https://thenextweb.com/security/2019/08/16/google-study-says-people-are-still-using-old-passwords-after-being-compromised/

5 Conclusion

Looking back at just two of the recent large data breaches in US history, the response of the companies leaves much to be desired. Hiding the breach, as in the case of Uber, or fumbling with letting users know who had been affected, as with Equifax, does not inspire confidence in those who we give our most confidential information. In this cyber-insecure world in which we live, the onus falls upon us as users to stay vigilant. While there are concrete consequences for the companies, the impact on victims is more nebulous – maybe your information will be sold and identity stolen, maybe your bank account will be drained, maybe private emails or photos will be released, or maybe it will aid the Chinese in their espionage data profiling of America. You don't ignore fraudulent credit card charges. Don't ignore fraudulent login attempts either.