

Facebook Not Protecting Employee Data Any Better Than It Does Customer Data

December 17, 2019 - Facebook and its subsidiaries have received a lot of bad publicity over the past year or so for customer data breaches. Some of those breaches were actually older - like the one with Cambridge Analytics that had to do with voter manipulation - and some more recent like those that involved customer data on Instagram and WhatsApp. These breaches resulted in the release personally identifiable information (PII) for millions of the company's customers. So you might think that the company would, at the very least, put out a memo telling employees that they need to be careful when handling PII, and a policy that limits access to that type of data to people with a need to know. Frankly, we don't know if the company put out such a memo. But we can say definitively that if they did, it didn't sink in.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
po.src = 'https://apis.google.com/js/plusone.js';  
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

One month ago today, a Facebook employee who worked in the company's payroll department decided to leave unencrypted hard drives in their locked car. Those drives contained PII on 29,000 Facebook employees. And that PII was extensive. It included names, SSNs, bank account numbers and overall earnings information. Additionally, it included information on the equity positions that individual employees have in the company.

In short, this is a bad breach. It contained pretty much everything and identity thief needs to assume someone else's identity and immediately drain their bank account.

In a statement, Facebook did say that they viewed the theft as a "smash and grab" theft and that ID theft wasn't a goal of the crime. They also said that the company had taken appropriate disciplinary action against the employee whose car was broken into. But all of that is probably little comfort to the impacted employees.

Anyone who thinks that their information was contained in this breach would be very well served to notify their bank and change their bank account numbers. Additionally, they should strongly consider freezing their credit files with Equifax, Experian and TransUnion.

Facebook realized that they had an issue on November 20th but the company didn't begin to notify employees until December 13th. Nothing like being timely!

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS