

Before Long You May Need to Take a Selfie When Making Online Purchases

October 20, 2017 - Banks and online merchants have been looking for ways to stop fraudulent transactions for years. The problem is especially prevalent for online purchases. As many as 18% of all attempted online purchases are denied; flagged as suspicious activity. But both Visa and MasterCard are working on platforms that will use biometric data to confirm the person making a purchase is actually the authorized card-holder. Those platforms are likely to change the way we all shop online.

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);  
})();
```

Biometric data consists of a lot more than a picture of your face. Fingerprints, voice recognition, retina scans—all of these are biometric. The term refers to your individual physical characteristics that can't be changed.

The new credit card platforms that will incorporate the use of biometric data will work like this. You make an online purchase on your phone. In order to authorize the purchase, the bank may ask you to take a selfie and then use facial recognition software to compare that picture to a picture they have taken of you. Or they may ask you to use your fingerprint to authorize the purchase.

When you are applying for new credit, it will probably become common place to have to submit a copy of your driver's license or a passport for facial recognition purposes, or perhaps a recording of your voice.

The goal, shared by both banks and merchants, is to reduce fraud by using information that can't be easily stolen in order to grant credit and authorize purchases. How well the plan will work though is debatable. From what we can see, there would be nothing to prevent an identity thief from using stolen data and his own picture or voice to apply for new credit. And once that's done, nothing to prevent that same identity thief from making a bunch of purchases. Of course, there is no telling how many identity thieves will be scared away by a requirement to provide biometric data to open new credit. It is also worth noting that the latest figures show that only 4% of identity theft involves the opening of new lines of credit.

The vast majority of ID theft involves criminals using existing lines of credit to make purchases. Biometric data authentication could make a significant difference here; perhaps stopping this form of identity theft in its tracks.

Consumers can expect to see the roll out of these biometric systems soon. MasterCard has already begun to issue new

cards that include a fingerprint sensor in them. The sensor is supposed to replace the need for a PIN when making a purchase. Not to be left out, Visa has also begun roll out of its platform and consumers are likely to start seeing changes within the next year.

While all of this is positive news for identity theft, it also raises some disturbing privacy issues. Specifically, there will soon be a lot of companies that are storing our biometric data. How are they going to protect that data? And what are the ramifications if that data is breached? None of that is clear right now and current laws regarding data breaches and data security don't appear to adequately address these issues.

byJim 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 me on Twitter:

Follow ACCESS