AMERICAN MARKETER

Business at its best

COLUMNS

Retailers must eye consumer privacy with secure payment methods

January 4, 2018

Yana Zaidiner is cofounder and chief operating officer of Token

By Yana Zaidiner

The majority of retailers use an online payment system to increase sales and consumer experience. Last year was known as the year of data breaches, with shoppers across the world losing private information, from social security numbers to credit card numbers and personal contact information the list goes on.

In an ecommerce and mobile world where data is easily compromised, retailers and brands need to make digital safety a priority and uphold a higher standard for financial security and privacy for consumers.

Unfortunately, in today's world, we live in the age of controversy between security and convenience. We do most of our shopping online, and more of our products and services are provided online than ever before.

Basket case
This move to online was facilitated by efforts from large online retailers to encourage the checkout process.

For example, shoppers constantly come across this option on many retail sites: "For your convenience, save your credit cards." Over time, saving a credit card to an account became the norm, especially with big online retailers where we shopped frequently and were encouraged to save card information. It made online shopping, in the shoppers' eyes, a seamless experience.

But with every online or in-person purchase, we have provided our sensitive payment information to the retailer. That retailer then stores our data in their database, and we in many ways have lost control of where it goes and with whom it is shared.

The reality is that security is only as strong as the weakest link in the chain, and the longer the chain, the more likely there is for a weak point.

As retailers grow, they have more employees, partners and contractors who need access to that information. Their information systems become more complex, and with that complexity, comes risk.

So, is the solution to avoid providing information to retailers?

In the store
As technology continues to advance, that option is unrealistic and will slow down the economy, at large. The problem is not so much how we give away data putting it in online or over the phone but how it is stored once we give it away.

The main and rather unfortunate lesson to keep in mind is that even the big, seemingly secure companies are just as much at risk as the smaller ones perhaps even more so because they hold more data and are therefore more attractive targets.

Think about the Uber hack that was recently reported, or Equifax's data breach. Even these institutions of commerce, which feel as though everyone uses them or everyone trusts them, cannot guarantee data security.

This leads to an ongoing tension between convenience and security.

For example, businesses are making it easier than ever to store your credit card information to an account in their application or on their Web site, streamlining the checkout process think Amazon, Uber or various airlines but data hacks have been more frequent than ever in the history of ecommerce.

While our first instinct is to hold merchants accountable and do not get me wrong, they are responsible for securing their databases we must remember the primary function of an online store or service provider is not data security. It is selling merchandise.

Would you buy a dress from a security company? Then why should we expect top-of-the-line security from a clothing store? That is why banks, credit card and technology companies are most likely going to lead the future of payment security.

The payoff
Take Apple, for example.

Apple Pay seeks to solve the problem of payment security by tokenizing credit card information each time you buy in a store.

When you buy something with Apple Pay, the store you purchase from receives a token as a representation of your credit card rather than your actual card number. Your card is still charged and the store does not know the difference, but your real credit card number is never provided to the store and ultimately never stored in its central database.

There is not quite a one-size-fits-all solution to solve the ongoing issue of securing our digital identities.

The best approach that business can have to protect consumer payment information is to not centrally store data. Business can work with security companies to tokenize data. However, this tends to be a costly project that often takes time.

The most efficient and secure solution would be for businesses to encourage consumers to pay with more secure payment services such as prepaid cards that are anonymous or use payment security solutions such as PayPal or similar applications that act as intermediaries and protect your payment information.

The solution for everyday consumers is to take more ownership over where we store and when we share our credit card information.

Sign up for options such as Apple Pay, PayPal or any other payment security solution.

Many of these solutions are perhaps advertised as convenience measures for example, "Create an account and check out with one click!" because it is easier to advertise and talk about than data security. But by understanding the function behind some of the services, we can see that they are also great protection mechanisms.

THE MORAL here is to stay aware.

Review your bank account daily. It does not have to take long. You know your habits, so unique charges will jump out to you. And use self-protective technologies to proactively protect yourself from next data breach.

Yana Zaidiner is cofounder and chief operating officer of Token, a New York-based mobile application that allows consumers to shop securely by disguising their payment details. Reach her at yana@jointoken.com.

American Marketer is published each business day. Thank you for reading us. Your feedback is welcome.