AMERICAN MARKETER

Business at its best

COLUMNS

How behavioral authentication can reduce fraud during the holidays

November 28, 2017

Deepak Dutt is founder/CEO of Zighra

By Deepak Dutt

Large-scale data breaches have become the new norm. Consumers lost $16 billion to identity theft or fraud in 2016, according to Javelin Strategy & Research.

Breaches that affected upscale retailers, including Saks Fifth Avenue and Brooks Brothers, serve as a stark reminder that the retail industry continues to suffer.

With the growth of ecommerce, mobile commerce and EMV at point-of-sale (POS) systems, data breaches are expected to get worse.

Pinning the problem

Major retailers are failing to keep up with critical processes needed to protect shoppers, who are left vulnerable to consumer fraud. Concerns are resurfacing as ecommerce merchants are expected to be hackers' prime target heading into the holiday shopping season.

New research reveals that mid- to large-sized ecommerce retailers face higher costs of fraud than smaller outlets that see less than $10 million in ecommerce sales.

For every dollar of fraud, these retailers incur $3.37 in costs that include chargeback fees, merchandise replacement and employee costs.

With high fraud costs, retailers are taking proactive measures to strengthen authentication methods and controls ahead of the holidays to ease consumer fears.

But hackers are getting more sophisticated and can easily access centralized company databases filled with credit card numbers, drivers' licenses, emails, phone numbers and more.

Following this year's string of breaches and malware attacks, methods such as passwords, pins and fixed physical characteristics such as fingerprints are not enough to secure consumer information.

Instead, more layers of information and the right combination of tools will be required to create a seamless, more

Instead, more layers of information and the right combination of tools will be required to create a seamless, more secure shopping experience.

Making sense

As we move into a sensor-based world driven by smartphones and other Internet of Things (IoT) devices, the future of mobile and online payments will lie in behavioral authentication, significantly reducing consumer fraud during the holidays, and beyond.

Behavioral authentication, or behavioral biometrics, is a form of biometric authentication that has shown promise in addressing the fraud problem.

Using artificial intelligence (AI) and machine learning algorithms, the technology quickly and continuously learns patterns of user behavior based on the way they interact with their devices muscle memory users exhibit while doing common tasks such as type, swipe and tap, to the hand they prefer to hold their device in rather than relying solely on fixed physical characteristics. It also takes into account a user's context such as type of device and geolocation.

Those factors are then analyzed to build highly accurate, personalized models of human behavior to verify that user's identity, differentiating between true users and fraudsters.

With hackers increasingly turning to machine learning and automated bots that mimic human qualities and actions to commit fraud even going as far as putting items in shopping carts behavioral authentication can even differentiate between humans and bots, precisely.

Behavioral biometrics ensures the security of the user and device when making a transaction through an online POS system, or mobile retail or payment application.

Behavioral biometrics protects against account takeover, automated bot attacks and other threats throughout a transaction, from start to finish.

The technology picks up on even the smallest deviation in normal behavior and flags it immediately to a business as a potential fraud attempt.

Instead of prompting consumers to enter their username and password, or scan their fingerprint, their implicit behavior is used as a silent authenticator to determine whether the user or a bot is trying to use the device, such as holding the phone and swiping across the screen.

Bio data

Behavioral biometrics phases out the possibility of a single password becoming a security flaw.

A hacker may be able to crack passwords, duplicate fingerprints and irises, and bots may be able to mimic human behavior. But it is virtually impossible to replicate the behavioral signature of a true human consumer in real-time.

This technology not only helps retailers and payment providers protect user information from ill-intentioned actors, but it eliminates the burdensome process of complicated passwords and extra security questions.

These tedious steps frustrate customers and oftentimes drive them away, causing retailers to lose business. Rather, it offers a frictionless experience that will not disrupt a consumer's normal routine.

Meanwhile, retailers and credit card companies are able to detect potential fraud or attempted identity theft with much greater detail.

BEHAVIORAL BIOMETRICS will play an important role in fighting fraud.

Adaptive AI engines, coupled with multiple layers of consumer behavior and user-device interactions will bolster authentication methods for retailers and payment companies alike.

Sophisticated user models will invisibly fit into existing architectures and business models without adding unnecessary friction to the consumer experience or business operations, all while deterring fraudsters.

Deepak Dutt is founder/CEO of Zighra, Ottawa, Ontario, Canada.