retail TouchPoints

PAYMENT AUTHENTICATION AND IoT DEVICES: DO MERCHANTS NEED TO PREPARE FOR FRAUD THROUGH REFRIGERATORS?

Written by Tim Sherwin, ***CardinalCommerce***

Perhaps the greatest revolution in shopping was the rise of e-Commerce. No longer were people required to physically go to stores to purchase goods; they could do so from the comfort of their own home on their computer. Today, we are experiencing a new shift in shopping and purchasing behaviors, and this time, shopping is leaving the computer and headed towards our appliances.

The rise of the smart home is here. And, while we still may be some years away from a mass-market refrigerator that refills itself through digital ordering, we've begun to see the beginnings with tools introduced by e-Commerce retail giants, such as smart speakers accompanied by virtual personal assistants. This impending networking of the home poses an interesting, if odd, question: can we trust our household appliances?

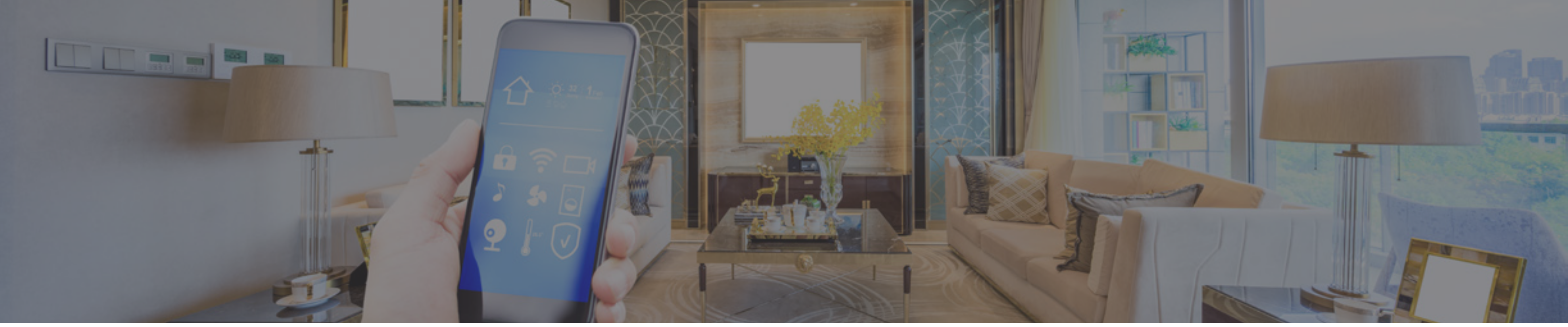
To phrase the question more clearly (and less ominously), can consumers and business owners trust the credit card and payment information that is contained within smart home devices?

The concept of the "Internet of Things" has long been criticized for leaving users of the technology and their personal information exposed. While it has greatly innovated traditional home appliances, these IoT devices often do not meet the necessary cybersecurity standards. Consumers that trust these Internet-connected devices can be left in the lurch as there is no barrier to prevent cybercriminals from hacking into these devices and accessing personal info.

E-Commerce merchants need to remain vigilant to this particular brand of fraud, as cybercriminals could be making purchases through their sites with fraudulent payment information, or perhaps even placed through someone's connected device without their knowledge.

How can merchants authenticate consumers' transactions when they are ordering a meal or household item by voice through connected devices? How can these transactions happen without fraud and without onerous input from the consumer? The answers to these questions lie in a new and improved protocol — 3DS 2.0 — technology that allows for a device-agnostic payments ecosystem.

Authentication is the means by which merchants and banks determine that a user attempting to make a digital transaction with a credit or debit card is, in fact, the holder of that card. Today, credit/debit card issuers in the U.S. that use 3DS solutions are relying on an updated version of the original authentication protocols that were developed in the early days of digital commerce.



Called 3-D Secure or 3DS, this set of authentication protocols establishes the standards by which card-issuing banks and merchants communicate to verify that the person conducting the transaction is the cardholder.

Unfortunately, when 3DS originally launched, there were several challenges that caused some retailers to lose faith in 3DS authentication, choosing to attempt other, lesser means of fraud protection. This is not an ideal situation, as without 3DS the financial burden of a fraudulent payment claim lies with the merchant, as it is uninsured by banks.

Payments industry group EMVCo. released the specs for 3DS 2.0, an update to the existing protocol 3-D Secure, in late 2016. Unlike the previous protocol, the new 2.0 authentication protocol was designed with IoT in mind, by increasing the number of data fields available to merchants who are confirming the identity of the cardholder. It's device-agnostic, so whether the consumer is using a wearable, a gaming device or an IoT device, they're able to check out/make purchases without friction.

3DS 2.0 offers substantial improvements, including giving merchants control over the checkout process and dramatically enhancing the amount of data that is used to perform authentication. This, in turn, decreases fraud and reduces false positives. In addition, authentication through 3DS 2.0 takes place almost completely in the background so consumers can complete their purchase without interruption.

As devices become more sophisticated and more prevalent, we can expect to see new challenges arise. However, the reduced friction afforded by 3DS 2.0 coupled with a connected device ecosystem presents an optimistic future for merchants, where payments can take place at anytime, anywhere, from any device. Opportunities are plentiful for merchant retailers that take the right approach.

retail TouchPoints®

Retail TouchPoints is an online publishing network for retail executives, with content focused on optimizing the customer experience across all channels. The *Retail TouchPoints* network is comprised of a weekly e-newsletter, special reports, web seminars, exclusive benchmark research, an insightful editorial blog, and a content-rich web site featuring daily news updates and multi-media interviews at **www.retailtouchpoints.com**. The *Retail TouchPoints* team also interacts with social media communities via Facebook, Twitter and LinkedIn.

CARDINAL® COMMERCE