CNP WHITE PAPERS

The Winding Road Toward IoT Commerce: Considering the Opportunities and Risks of Selling Through Connected Devices

CNP CARD NOT PRESENT®
NEWS, EDUCATION AND EVENTS
DECODING DIGITAL PAYMENTS & FRAUD

Radial
a bpost company

Table of Contents

Introduction

In May of 2018, a woman contacted Seattle television station KIRO with a story that became the first truly public skirmish in a war merchants will be fighting more and more as they seek out new sales channels. Digital home assistants had been one of the most popular gifts during the previous holiday season—a manageable first step toward making the connected home of the future a reality for many consumers. But the local news report and national interest it subsequently generated are one facet of the challenges merchants will face as they turn to the Internet of Things (IoT) to reduce friction in online transactions.

An Amazon Echo device in the woman's home recorded and sent a lengthy private conversation to one of her husband's employees. An investigation by Amazon found the device had misinterpreted regular conversation as commands to wake up the device and send a message (the ensuing conversation) to one of the contacts stored in the device.

The episode was widely covered in the media. And, while Amazon concluded the cause was accidental rather than malicious, it showed how consumers will react to security concerns when the territory is unfamiliar—and how the media's coverage of that reaction can slow adoption of a potentially lucrative sales channel.

Regarding commerce, IoT currently is all beautiful potential. The most oft-quoted statistic illustrating that potential comes from Gartner. Last year, the research and advisory firm based in Stamford, Conn. predicted 8.4 billion connected things would be in use by the end of 2017. And, by the end of 2020, that number will grow to 20.4 billion[1].

1. Gartner Says 8.4 Billion Connected 'Things' Will Be in Use in 2017, Up 31 Percent From 2016 – Feb. 2017, Gartner

The cars, smart TVs, wearables, digital home assistants, appliances, thermostats and other products that consumers are buying today increasingly are connected to the Internet, enabling automatic, seamless communication of data between machines that greatly reduces the need for human intervention. This communication, at its best, will allow machines to do better what they have always done: give time back to people who before would have had to operate them or do the work manually.

> *"The number of devices that will be involved means the threat landscape is much bigger than anyone can feasibly handle right now..."*

At the moment, however, most of that potential remains untapped. Ideas for engaging in online commerce via Internet-connected devices abound. But, reliable numbers of actual sales completed through these devices are scarce. One study that examined voice shopping said e-commerce via digital home assistants like Amazon Echo and Google Home in the U.S. market totaled $2 billion in 2017[2]. Considering U.S. consumers spent more than $450 billion online that year, IoT purchases are off to a modest start.

There are billions of connected devices in use, however, and, as Gartner and others predict, that number will quickly double and growth figures will accelerate. The connected infrastructure is waiting for retailers and technology providers to leverage it, turning it into rich, frictionless shopping experiences. And, while plenty of innovators are thinking about, and working on how to deliver those experiences, experts say relatively few are thinking about the associated risks.

If those concerns are not addressed by companies interested in supporting shopping via IoT, the potential scale of connected commerce could result in a significant increase in card-not-present fraud. In addition to the financial loss companies might incur, insufficient attention to security also could lead to other incidents like the Amazon mishap in Portland resulting in reputational damage and potential setbacks in consumers' trust in the new channels.

As commerce via the IoT proliferates, it will further complicate an already complicated ecosystem. Merchants must begin to consider now how their e-commerce environments will change.

2. The Talking Shop: the Rise of Voice Commerce – Feb. 2018, OC&C Strategy Consultants

Data: Boon and Curse

One of the reasons e- and m-commerce have flourished is because, as consumers began to first use the PC and then the smartphone to shop for and buy things, they both provided platforms for two-way communication. That communication has resulted not only in remote channels to push out sales, but also a return of data enabling increasingly customized and engaging shopping experiences for individuals.

The effect of IoT on data creation will be profound. The amount of data produced each year will increase from 218 zettabytes (ZB) (a zettabyte equals 1 trillion gigabytes) in 2016 to 874 ZB by 2021, according to Cisco[3]. The increase will be driven almost entirely by the increase in devices connected to the Internet, the company said.

> *"The amount of data that is going to be available and streaming into merchants that are looking at customers who are performing transactions with IoT devices is going to be huge... The primary thing people need to be aware of is the amount of data they deal with today and the storage they have set aside for it will simply not be sufficient moving forward."*

While businesses will each only deal with a small fraction of that global output, in order to fully take advantage of the opportunity the IoT presents, those that want to support it will need to consider significantly upgrading their ability to handle the expected deluge of data. Most, however, are not effectively preparing for it, according to John Venglass, senior product manager for Payments & Fraud at omnichannel technology and operations services provider Radial.

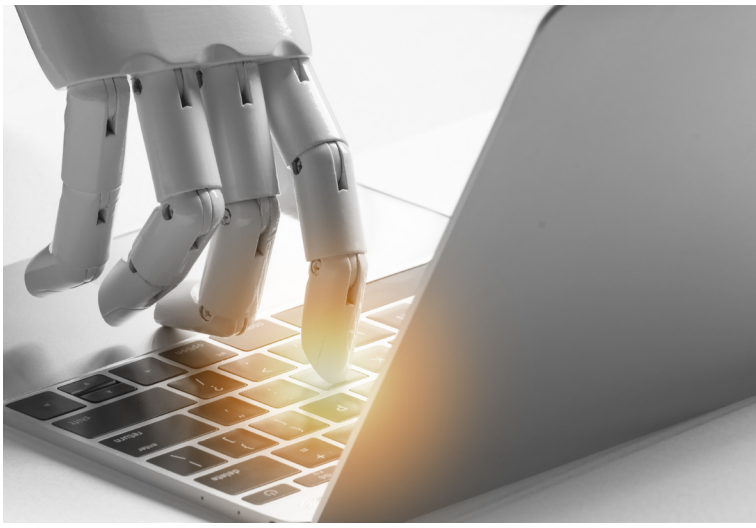
"The amount of data that is going to be available and streaming into merchants that are looking at customers who are performing transactions with IoT devices is going to be huge," Venglass says. "The primary thing people need to be aware of is the amount of data they deal with today and the storage they have set aside for it will simply not be sufficient moving forward."

Businesses that will support IoT purchases first and foremost should consider increasing their data storage capacity at least by a factor of five to handle the information that will be generated by those customers.

3. Cisco Global Cloud Index – Feb. 2018, Cisco

Capturing as much of that data as possible will be important for designing compelling and engaging experiences. Unfortunately, the very act of introducing data flow from so many additional sources vastly expands what security professionals call a company's "attack surface." And, as Venglass notes, neither payments and fraud technology providers, nor merchants themselves, are working on specific solutions to address exposure to the increased attack surface created by IoT.

Bots and Botnets: Turning Our Devices Against Us



Once merchants begin to get a grasp on how the enormous proliferation of connected devices and the data they generate affects their exposure to security events and fraud, they can begin to think about the specific shape those threats will take for their businesses.

Just about every technology employed as a new channel in the name of commerce has been leveraged in innovative and unpredictable ways to steal from the merchants doing the selling or the consumers doing the buying. Criminals undoubtedly will do the same thing with IoT devices, but one particular threat has emerged as the top concern: the ease with which bad actors can infect IoT devices with malware.

With billions of connected devices in operation, the potential for someone to hijack a subset of them and use them as a powerful botnet to inflict damage on a specific site or across the Internet is enormous. In fact, according to Bernard McManus, head of global fraud management and strategy for Playstation, right now, it's the primary threat.

"You're talking 18 billion connected devices today and it's going to go up to 70 billion by 2025," McManus notes. "That's 10 to 20 devices per household that connect with the Internet and can be infected with malware. A lot of them will be doing commerce, but I don't necessarily think the vulnerability comes from that. I definitely think they can be used as proxies or bots to do all sorts of malicious activity."

McManus highlighted the Mirai botnet from 2016 as an example. He describes it as the biggest denial-of-service botnet ever.

"That's what you're up against," he says. "If there's a large IoT botnet attack during Black Friday or Cyber Monday, it's going to be very hard to keep your website up and running. I don't think a lot of companies are taking the threat seriously enough."

Brett Johnson, a former hacker and Most Wanted criminal who was a founding member of one of the first online forums where criminals and fraudsters shared tactics and sold stolen information, agrees.

"The number of devices that will be involved means the threat landscape is much bigger than anyone can feasibly handle right now," he says.

In addition to DDoS attacks, Johnson says cybercriminals can use IoT devices they have taken over for activities like geo-location spoofing, installing ransomware, placing fraudulent orders or engaging in account takeover fraud.

Digital Goods Sellers Beware

McManus is accurate that IoT commerce is still nascent. But, as Johnson suggests, the bot activity they describe is not limited to security events like DDoS attacks and installing ransomware. Enough merchants are supporting online transactions through connected devices other than PCs, smartphones and tablets that fraud attacks are occurring now. And, as the popularity of the channel grows, the fraud will grow along with it.

Karisse Hendrick, principal at fraud consultancy Chargelytics Consulting, says fraud professionals at merchants that support IoT transactions—especially those that sell digital goods—are reporting increased activity through the channel.

> *"Unlike mobile phones, tablets and PCs, very little security has been built into IoT devices, nor is anti-malware software available for them... Using bots, criminals are placing orders through everything from digital assistants to refrigerators to smart home security devices."*

"Unlike mobile phones, tablets and PCs, very little security has been built into IoT devices, nor is anti-malware software available for them," Hendrick explains. "They're susceptible, therefore, to being used as bots to place orders. Using bots, criminals are placing orders through everything from digital assistants to refrigerators to smart home security devices."

Accepting orders that originate from IoT devices will be an important part of generating revenue growth in the future, so blocking all transactions from IoT devices is not a feasible antifraud strategy going forward. Defending against fraud through online channels will have to evolve.

Unfortunately, one popular tactic that intuitively makes sense as a way to identify an IoT device being used as a bot to place online orders is not available to fraud fighters. Many merchants rely on device ID information to prevent one device from making multiple orders with different payment credentials.

"Current technology makes obtaining a device ID from a specific IoT device impossible," Hendrick notes. "Until the security technology imbedded in connected things improves, some familiar ways of evaluating online transactions for legitimacy are not accessible. Awareness of challenges like these will enable fraud managers to spot patterns pertaining to orders from IoT devices. If you suddenly see a large uptick in orders coming from refrigerators and you're a money transfer service, you should probably be suspicious."

Avoiding an Alexa Moment

For companies interested in expanding their revenue via the new channels opened by IoT, considering the security and fraud concerns inherent in new technologies is a must. Security is the top impediment to adoption of any new technology used to make payments, according to Al Pascual, research director and head of Fraud & Security at Javelin Strategy & Research.

And, if something goes wrong early in the product lifecycle, for instance, a conversation recorded by a digital home assistant that is sent without a user's knowledge to a recipient in another state, unwelcome media attention could negatively affect adoption and stunt the effectiveness of the new channel.

"The challenge becomes that we see things in the media more often about the lack of security, both in the channels in which we already play (e.g., e-commerce and banking) and especially in newer channels where businesses want us to interact with them."

Pascual points to an early Apple Pay glitch that enabled criminals to easily load stolen payment credentials into iPhones as an event that may have had an effect on mobile payments in the U.S., which lags other places in the world. More events like the Alexa mishap that are captured in the media could affect the number of people who are willing to make purchases on an IoT device. And, right now, a Javelin report shows that even most people who own an Amazon Echo or other IoT device are not comfortable using them to make payments yet.

Of the estimated 165.5 million U.S. consumers who own at least one IoT device, Javelin found that more than two-thirds report they would be skeptical of making a payment via that device[4].

Conclusion

Billions of connected devices already exist in the homes and cars of consumers worldwide. Delivering incredible shopping experiences using those devices is already on the roadmap for many companies. The data those devices will generate, while it will be the basis for many of those experiences, will present a multitude of problems.

Storage of the data will be an issue, as will the proclivity of bad actors to access, use and monetize that data illegally.

"This large increase in data will necessitate not just more storage, but also more processing power to compare all of these additional data elements within a fraud provider's systems," Radial's Venglass points out. "Finding the fraud links once data has grown to 4 or 5 times the current volume is going to really tax these platforms."

Whether it means preparing to handle, analyze and leverage that data using in-house resources or partnering with third parties that can help, smart companies are bolstering their e-commerce environments now for a future in which sales through IoT channels become a major revenue contributor.

4. Securing Emerging Channels: Virtual Assistants, The Internet of Things, and Beyond – July 2018, Javelin Strategy & Research

ABOUT CARD NOT PRESENT®

Card Not Present, part of the RELX Group, is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. The company's media platforms include the CardNotPresent.com portal, the hub for news, information and analysis about the payments issues that most affect merchants operating in the space; the CNP Report, an e-newsletter delivering that focused information directly to your email inbox twice a week with no extraneous clutter; the CNP Expo, an annual gathering of the leading companies in the space from the smallest e-commerce Websites and technology providers to global retailers and payment processors; and the CNP Awards, an annual event honoring the products and solutions CNP merchants rely on most to increase sales. For more information, visit CardNotPresent.com.

ABOUT RADIAL

Radial brings more than 15 years of experience and 24x7x365 resources that work in concert and adjust in real time to ensure cyber criminals don't get the upper hand. We are committed to our clients' success including indemnifying fraud — even for high-risk markets — and only charging for approved orders. Flexible options allow merchants to leverage the solutions that best meet the needs of their organization whether it's for complete fraud management for all orders, fraud management for high-risk orders only, or a risk rating to supplement a merchant's existing tool set. We are obsessed with fraud so merchants don't have to be. Radial's omnichannel technology and services also include order management, store fulfillment, logistics, dropship, and customer care. Learn how we work with you at www.radial.com.

This document was produced as a joint effort between Card Not Present® and Radial.

CNP CARD NOT PRESENT®
NEWS, EDUCATION AND EVENTS
DECODING DIGITAL PAYMENTS & FRAUD

Radial
a bpost company