CASHNet®
Payment Solutions
Provided by Higher One®

2016

Payment Technology Predictions for Higher Education

2015 Recap

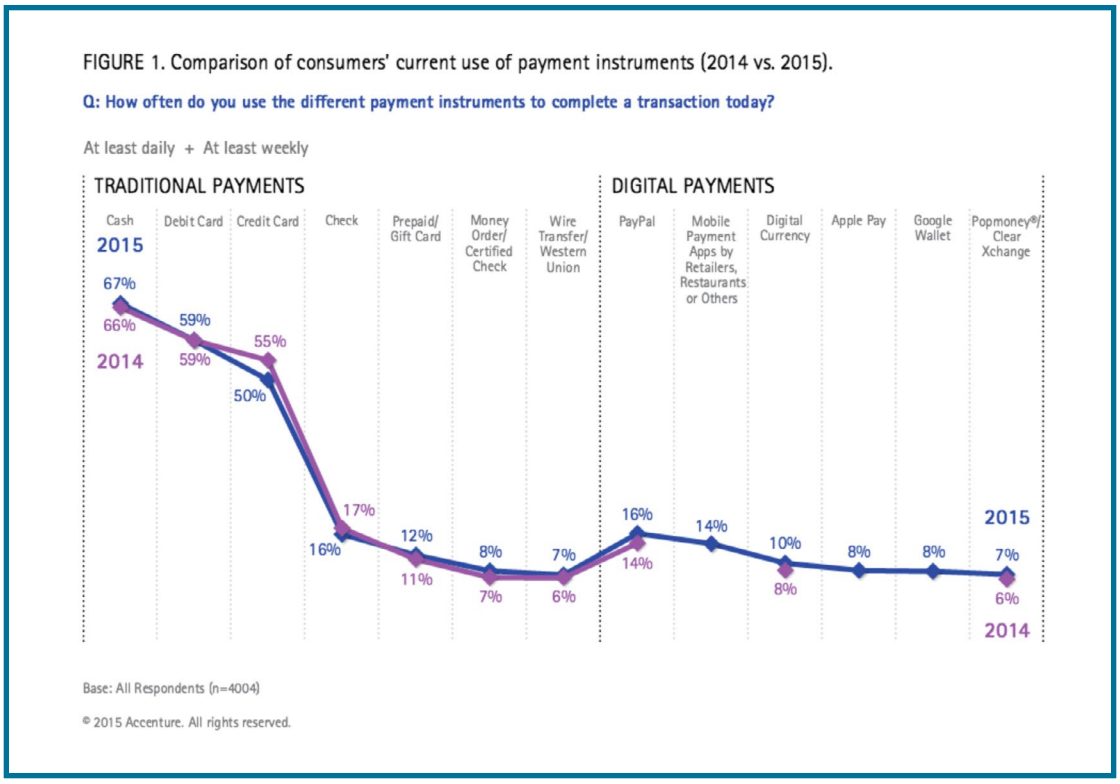
The 2015 payment technology landscape generated significant buzz with regard to data security, digital wallets, digital currencies, and peer-to-peer (P2P) technologies. It was quite eventful to say the least. Also with the big liability shift date for EMV, there was a definite heightened sense of anxiety and significant level of confusion for merchants and payers alike. Still, we remained focused on bringing our clients the latest industry news, updates and information for everything that might have impacted their students or campus.

To quickly recap 2015's hot topics:

The EMV rollout was top of mind for nearly everyone as merchants, issuers, and consumers were all impacted in some way during this implementation. Payment vendors increased their efforts to educate the market about EMV and raced to become EMV-certified, before realizing that the process was actually more arduous than originally anticipated. With some of the largest retailers (i.e. Target and Walmart) having had success with a full rollout before the end of year, even they missed the October 1, 2015 liability date. Everyone else was left to be patient and work through the process. The silver lining for higher education is that in most cases the risk of card-present fraud is very low. As such, most higher education institutions are in a position to define their EMV strategy by asking some key questions like:

- How many devices will you want to replace?
- How much will it cost to replace these devices?
- What is the total volume of card-present fraud you experience on campus?
- When would it be advantageous to replace devices? (Keep in mind training, peak volumes, etc.)

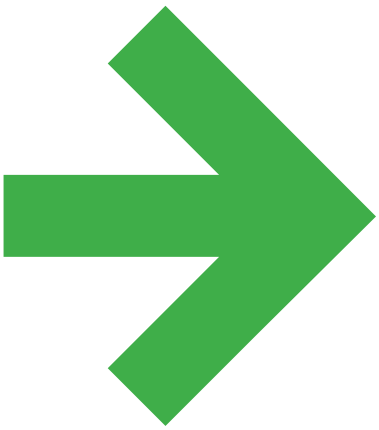
Digital/mobile payments experienced growth. According to a recent Accenture survey, while 52% of North Americans are "extremely aware" of mobile payments, only 18% use them on a regular basis.[1] Millennials and higher-income households lead with 23% and 38% using contactless payments at least once a week, respectively. Still, we saw a notable growth in every category of digital payments, including healthy usage percentages for technologies that didn't exist in 2014 like mobile payment apps by retailers, Apple Pay® and Google Wallet™ (Android Pay™). This growth was partially bolstered by the impact of the EMV implementation, and the new NFC-compatible hardware that was being installed to accept EMV payments.



Increase in high profile breaches. According to ITRC, a nationally recognized non-profit organization which provides victim assistance and consumer education through its toll-free call center, 2015 was the second highest year for data breaches since they started recording them in 2005, with a total of 781 publicly recorded breaches.[2] Forty percent of the reported breaches targeted the business sector while the education sector made up 7.4%. The most important to note is that 2015 reached a nine-year high for hacked incidents, up 8.4% over 2014, which often made mainstream news, thanks to our socially connected world.

Consumers and merchants sought a deeper understanding for securing sensitive data. Since many of these breaches were reported in mainstream media, there were heightened concerns of possible reputational damage for institutions. For consumers, these attacks were troublesome as they caused fearfulness regarding the handling of confidential consumer data. (As a result, we have noticed an increase in webinar attendance as clients looked for best practices on how to safeguard against possible breaches.)

As we enter the third month of 2016, we want to share our list of a few topics that will be important for higher education institutions to keep a pulse on for the coming year.



2016 Predictions

1. An increased focus to mitigate card-not-present fraud.

As EMV terminal adoption increases, so will online, card-not-present fraud. This has been the case in nearly every market that has gone through the EMV implementation prior to the U.S. One market to prove as a point of reference is France's move to EMV. While it helped reduce card-present fraud by 35% during 2004-2009, it simultaneously experienced an increase of 360% of card-not present fraud. In the U.S. the Aite Group predicts that card not-present fraud will more than double to a total amount of $6.3 billion.[3] While fraudsters will gravitate toward the path of least resistance in the wake of the EMV implementation, the increase of card-not-present fraud is often amplified by an increase in payment volume for online payments. Companies continue to look for ways to mitigate this fraud risk through the introduction of new technologies by most likely using a combination of approaches. While early attempts have focused on biometrics to help fight this fraud, in 2016, look for the introduction of dynamic data in the card-not-present transaction flow. In addition, research is being done on consumer behavioral data in the hopes that it will help authenticate the payer without adding friction to the checkout process.

2. Near field communication (NFC) will continue to work to define a value proposition to increase adoption.

While NFC payment usage has increased, it still represents a minority of POS payments. There are a number of factors that contribute to the relatively low payment volume, but perhaps the largest factor is the lack of a compelling value proposition for the payer to change an ingrained habit. For students, this change may get a boost from a seemingly unrelated source. According to a recent survey taken by SmartCard Alliance, there are already several non-payment uses for NFC. Three higher education campuses have piloted experiments leveraging NFC technology to unlock doors (including dormitories) replacing the need for student IDs with contactless chips. The three campuses have reported benefits that include a decrease in replacing lost/stolen ID cards, and a significant decrease in spending to replace the door locks every year.[4] By making students more reliant upon their smartphones for entry into campus buildings, could these programs prompt students to be more reliant on these same smartphones to make purchases with their NFC-enabled virtual wallets? On top of this, retailers are getting more creative by offering consumers rewards for using NFC.[5] Walgreens recently announced its partnership with

Apple Pay for its loyalty program. In 2016 look for new value propositions to emerge for NFC enabled wallets, and consequently payment volume through these payment vehicles to increase substantially with Millenials.

2016 will continue to be a year of rapid development for the payment space as the industry churns out new technologies to decrease friction at the point of sale and mitigate the growing risk of fraud. You can continue relying on the CASHNet® team to keep you informed of industry trends and help ensure successful campus payment experiences.

Sources:

1. https://www.accenture.com/t20151021T165757__w__/us-en/_acnmedia/Accenture/next-gen/na-payment-survpdfs/Accenture-Digital-Payments-Survey-North-America-Accenture-Executive-Summary.pdf
2. http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html
3. http://www.paymentssource.com/news/paythink/ecommerce-fraud-could-get-really-bad-post-emv-3021286-1.html
4. http://www.smartcardalliance.org/wp-content/uploads/NFC-Non-Payments-Use-Cases-v23-121715-clean.pdf
5. http://fortune.com/2015/10/29/mobile-payments-grow-2016/