SPRING | 2018

Bank of America
Merchant Services

SpendTalk

The latest payments, eCommerce, fraud and security trends from Bank of America Merchant Services

Welcome to SpendTalk

from Bank of America Merchant Services

At Bank of America Merchant Services, we're often asked for our perspective on the trends that are reshaping global commerce and, specifically, payments. Throughout the year, in face-to-face meetings, publications and industry forums, we eagerly offer up our proprietary analyses and insights to help businesses make sense of rapidly evolving changes in consumer behavior.

SpendTalk is a new seasonal publication from Bank of America Merchant Services that will share our take on a number of these trends. In this inaugural edition, we briefly touch on eCommerce growth patterns and spikes in spring spending by category, and dive deeper into the topic of fraud and how businesses are confronting ever-changing threats. We also summarize the four most-important takeaways from popular cybersecurity webcasts we hosted earlier in 2018.

Consider SpendTalk a springboard for discussion with your Bank of America Merchant Services business consultant. It's Bank of America Merchant Services' privilege to serve you and help your business stay on top of the latest payments, eCommerce, fraud and security trends. Let's keep the conversation going.

How enhancing your search and payment strategy can help you keep customers

Where eCommerce is concerned, the headlines don't lie.

A recent study by PwC found that online commerce channels grew at more than seven times the rate of the retail sector as a whole in 2016.[1] Bank of America Merchant Services' transactional data analysis confirms this trend. Even sectors previously resistant to eCommerce forces — restaurants, grocery and convenience stores — are seeing notable upticks in online sales growth.

The explosion of eCommerce is wholly transforming the way businesses and consumers interact. Now that websites, made-for-mobile apps and other technologies have made shopping faster, easier and more convenient, two points along the purchasing journey are proving to be particularly critical: search and payment.

Don't snooze on site search

Consumers are most motivated to buy when they search for a product or service on a business' website, so it's essential to deliver accurate, useful search results. Likewise, the payment process must also be fast and seamless or consumers will simply abandon their shopping carts—both online and in stores.

Research found many companies create unwanted friction in their online search functions with nearly 70 percent of the top 50 retail websites unable to return relevant search results for product synonyms.[2] Failing to meet customer expectations in this area can be especially costly since shoppers who perform in-site searches end up buying from that business at twice the rate of visitors who don't use search.[3] For this reason, improving search capabilities presents a huge opportunity for growth and differentiation.

"If you haven't optimized the search experience from start to finish, you're missing out on higher conversion rates and greater customer loyalty," said Michael Roberts, chief marketing and digital strategy officer at Bank of America Merchant Services.

Making payment an afterthought

Payment, like search, is trending toward less friction and greater speed. Yet the proliferation of new payment options can be difficult for both merchants and consumers to navigate. Mobile apps let consumers order a coffee—or a car—hours in advance, and make seemingly invisible, cashless payments on their mobile devices. Digital wallets let shoppers keep tangible payment cards in their wallet while they pay and provide centralized access to merchant rewards programs. With contactless point-of-sale (POS) terminals, paying for a purchase is as easy as tapping a phone. In the background, tokenization increases purchase security by substituting sensitive data with non-sensitive information.

The benefits for consumers are clear: more convenience and faster transactions. Companies benefit not only by remaining relevant and reducing swipe fees, but by creating a more personalized experience that increases customer loyalty and drives additional sales.

As consumers grow more sophisticated and demanding, businesses must keep up with their evolving expectations. That starts with aligning the consumer experience across multiple channels, making search easy and highly productive, and making payments as invisible as possible.

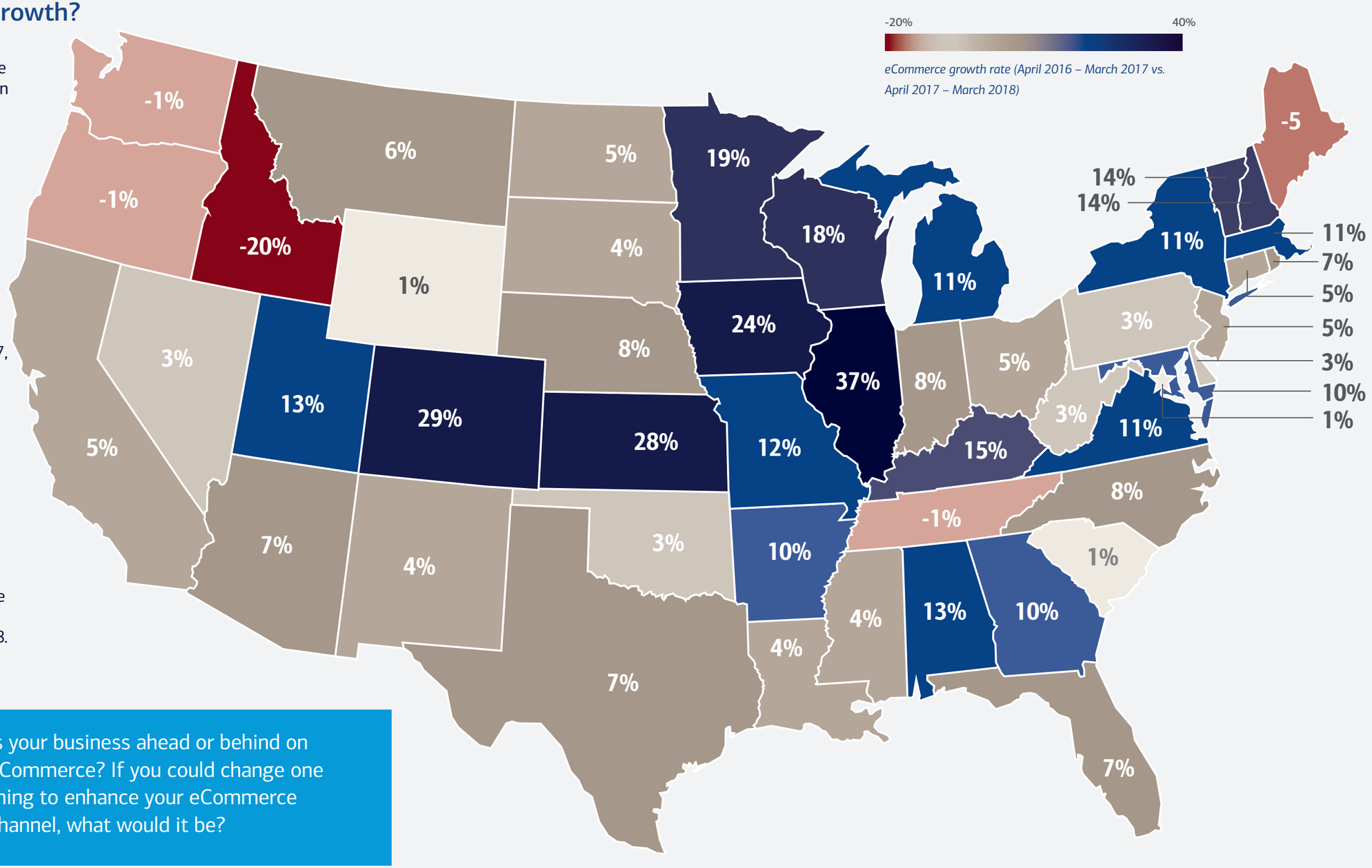
> "If you haven't optimized the search experience from start to finish, you're missing out on higher conversion rates and greater customer loyalty."
>
> - Michael Roberts, chief marketing and digital strategy officer at Bank of America Merchant Services.

Does your marketing strategy account for the differences in regional eCommerce growth?

Not surprisingly, the adoption of eCommerce shopping behaviors in the U.S. took initial root in America's urban and suburban regions — particularly along the coasts — where amenities like high-speed internet access first rolled out.

However, Bank of America Merchant Services' data shows that the eCommerce growth rate continues to outpace that of brick-and-mortar — particularly in middle America.

For example, Bank of America Merchant Services' data comparing the 12 months ending March 31, 2017, to the 12 months ending March 31, 2018, shows that eCommerce sales are outperforming brick-and-mortar sales at higher rates — ranging from 18 to 37 percent — in Illinois, Iowa, Minnesota and Wisconsin. By comparison, coastal areas like California, New York, Florida and Washington, D.C. witnessed rates of growth no higher than 11 percent, according to Bank of America Merchant Services data comparing the 12 months ending March 31, 2017, to the 12 months ending March 31, 2018. How fast has eCommerce grown in your regions?



THOUGHT STARTER

Is your business ahead or behind on eCommerce? If you could change one thing to enhance your eCommerce channel, what would it be?

Source: Bank of America Merchant Services data comparing the 12 months ending March 31, 2017 to the 12 months ending March 31, 2018.

Behind the numbers: Spring spending growth

Spring is here, which usually means consumers begin cleaning and improving their homes. But that's not all they are spending money on this time of year, according to spending at U.S. businesses that rely on Bank of America Merchant Services to help them process customer payments.[4]

March usually sees an uptick in overall sales volume across many segments of the economy following lower spending in the months of January and February as people recover from holiday splurges. Tax refunds and yearly bonus payouts are also a factor in how much they spend.

Three industries saw increases this year — just before and shortly after the start of spring: home improvement, clothing and travel. Here's a look behind the numbers.

Home Improvement

Consumers in the Northeast wait until the threat of snow diminishes before tackling home improvement projects. While March only saw about a 5 percent spike in sales in the Northeast, the warmer month of April saw six times that surge. By April, though, the growth trend leveled out across the country indicating that homeowners from coast to coast are undertaking home improvement projects.

Clothing

According to Bank of America Merchant Services' data comparing January and February to March and April of 2018, the southern U.S. saw a 36 percent uptick in spending on clothing beginning in March, far outpacing any other U.S. region. In contrast, the Northeast and the West saw a 42 percent and 23 percent boost, respectively, in April. This is likely due to the start of spring being the ideal time for consumers in these regions to begin shopping for warm-weather clothing. By April, the data indicates that consumers in the South have already made their purchases and have slowed their spending.

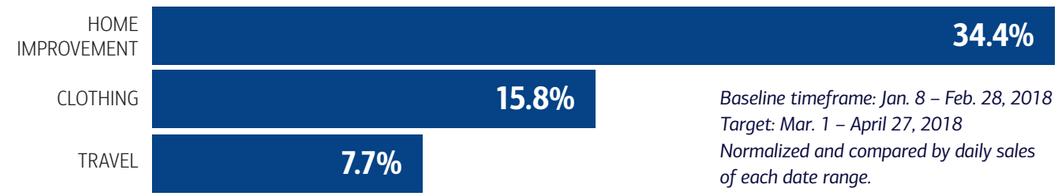
Travel

Cabin fever tends to set in by March and families start booking travel for summer vacations. In March, the southern and western U.S. became travel destinations — likely by vacationers from the Northeast and Midwest. By April, there was little difference in sales growth across the industry. Overall, travel spending growth was nearly 8 percent; this includes purchases at gas stations, airlines, cruise lines, hotels and other travel-related businesses.

Cruise lines saw more than a 14 percent increase over typical growth, which makes sense as consumers tend to book more expensive trips earlier in the year. Airline ticket sales only saw a 3 percent increase, which may mean consumers are waiting to book flights closer to their planned vacations.

FIGURE 1

Categories that see the most growth in the spring



Baseline timeframe: Jan. 8 – Feb. 28, 2018
Target: Mar. 1 – April 27, 2018
Normalized and compared by daily sales of each date range.

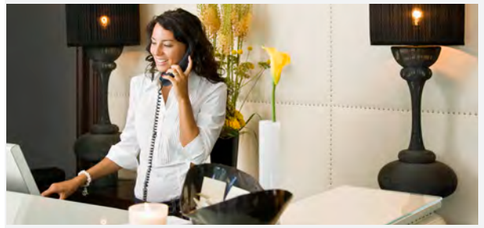
THOUGHT STARTER

Does your business see an uptick or pullback in sales during the spring? How does your business seize on seasonal consumer spending trends?

4 key takeaways from Bank of America Merchant Services' 2018 cybersecurity webcasts

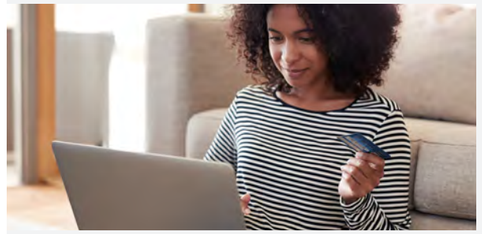
It is critical that businesses of all sizes take a hard look at how they monitor and protect customers at the point of sale — namely, customers' credit card data — online, in-store and on mobile devices.

In March, Bank of America Merchant Services hosted a series of webcasts designed to help businesses safeguard their data. Here are four takeaways.



1. Certain industries suffer higher data breach costs than others.

Any industry with a connected computer is a potential victim of a data compromise. Heavily regulated industries such as healthcare, education and financial organizations have higher per-incident costs. (See Figure 2).



2. Nearly 20 percent of consumers would permanently abandon a business that experienced a data breach.[5]

The customers that come back are still slow to do so. More than half believe it would take them at least three months to be comfortable enough to start shopping with that business again.

3. In 2017, the global average cost of a data breach was $3.6 million or $141 per data record.[6]

That's a reduction on the average cost from 2016, but the average size of data breaches has increased. It's also worth noting that the average cost of a data breach in the U.S. is much higher at $7.3 million.

4. A strong fraud strategy is important.

Businesses should consider all the ways they accept payments — both online and in-person — to ensure they are providing both themselves and their customers with the proper tools to minimize the impact of a potential data compromise.

FIGURE 2

Per capita data breach cost by industry classification in 2017

Source: 2017 Cost of Breach Study, Ponemon Institute[6]

Interested in learning more?
Visit merch.bankofamerica.com

THOUGHT STARTER

Does your business accept EMV-enabled chip cards? Have you considered using artificial intelligence (AI) or machine learning to better manage fraud?

Fraud is evolving. So should your data security.

Help safeguard your company and customer data at the point of sale

The fintech industry has made huge strides in data security, including wide implementation of EMV® technology and end-to-end data encryption. Yet these technologies alone aren't enough.

Chip card technology has reduced point-of-sale fraud — but bad actors are shifting their attention to card-not-present interactions such as online purchases. In fact, incidents of card-not-present fraud jumped 40 percent in the United States in 2016.[7] According to Juniper Research, card-not-present fraud alone could cost retailers $71 billion globally over the next five years.[8]

Evolutions in fraud demand a new generation of security solutions.

"Fraud isn't going away — it's getting more sophisticated," says Larry Brennan, senior vice president of merchant data security and cybersecurity at Bank of America Merchant Services. "But the security industry is always applying new techniques to keep pace."

Here's what you need to know about the current state of data security.

Fear factor: Skimming, shimming and smishing

Fraud aimed at stealing information from consumers and businesses is increasing, both online and on the ground.

Today's data thieves are using increasingly sophisticated phishing schemes to download personal information from computers, as well as "smishing" schemes that target mobile devices. Additionally, the growing availability of 3-D printing technology makes it cheaper and easier for data thieves to target customers at a business' physical point of sale, allowing for the quick creation of skimming devices (which fit over legitimate credit card readers to steal card data) and shimming devices (which fit inside card readers). Incidents of compromised ATMs and merchant devices rose 30 percent from 2015 to 2016, following a six-fold increase in 2015.[9]

After stealing personal and credit card data with these methods, criminals sell it to be used in card-not-present fraud. Such black-market data sales also have become more sophisticated. For example, cybercriminals bundle stolen credit card information from a single zip code and sell it in that area to evade security systems that monitor out-of-area credit card use.

> "Fraud isn't going away — it's getting more sophisticated."

The public and private cost of a data breach

Businesses incur a range of expenses when data breaches occur, including refunds for fraudulent purchases, penalties for noncompliance with EMV chip card standards and reimbursing credit card issuers for the cost of replacing cards, which can run more than $200 apiece.

Moreover, insurance companies after a breach may demand that businesses hire outside legal counsel or breach coaches

This Insight was originally published by Bank of America Merchant Services in late 2017.

to oversee security. (Cases where 30,000 or more cards have been compromised typically trigger such requirements.) Larger companies may also need to invest in a PCI forensic investigator to help pinpoint where the breach happened and prevent future attacks.

Merchants with compromised data also incur considerable public relations costs.

"Customers lose trust in a business after a breach," says Gregg Kambour, vice president of solutions consulting at Bank of America. "Canceling and replacing cards is directly disruptive to customers' lives."

Companies may have to hire PR firms to handle public announcements about the breach and to develop and execute campaigns to win back public trust. The expenses can add up quickly: Simply hiring a PR agency can cost $100 to $500 per hour, depending on the size of the firm. Putting the agency on retainer can cost from $1,000 to tens of thousands of dollars per month. Add the costs of direct mail campaigns, traditional and social media outreach and increased customer support, and the sums can reach staggering levels.

Evolving security solutions

Security threats evolve constantly, as do technology solutions.

"EMV is not a cure-all," says Brennan. Pair it and data encryption with tokenization to protect customer data further. Tokenization — which retrieves credit card data using randomly generated one-time tokens that carry no personal information — enables companies to remove credit card data from their internal networks.

"Technology companies like Bank of America Merchant Services are trying to provide a holistic view of fraud activities to beat down both card-not-present and card-present fraud," says Raoul Aranha, vice president, security, fraud and analytics services at Bank of America Merchant Services.

For example, security companies are:

- Developing machine learning systems that can track fraud before it occurs. Machine-learning software combs through company and online data to identify characteristics of fraud automatically. It looks for patterns in credit card use, identifies anomalies in those patterns and flags the anomalies as potential fraud activity.
- Building broad networks that share data on fraud. "Bank of America Merchant Services has access to issuer data, network data and merchant-acquiring data," says Michael Roberts, chief marketing and digital strategy officer. "That allows us to create models that will outperform company models that rely solely on internal data." These networks can alert merchants that a card making a purchase triggered a red flag at another retailer.

Protect your business—and your customers—going forward

Holding ongoing conversations about new developments with security providers and payment vendors, such as Bank of America Merchant Services, can help businesses apply emerging technologies that suit their size, industry and customer base. But a few basic preventative measures from within can help thwart data theft attempts. Here are two:

- Teach employees at the point of sale to search for skimming and shimming devices by looking for ill-fitting card reader covers at the beginning of every shift.
- Run training exercises and drills — covering scenarios such as a phishing attempt — so all employees are familiar with fraud tactics and alert to them, and know the roles they are expected to play.

Every company today must safeguard customers' data in the face of constant and evolving threats. Payment technology vendors are in a unique position to help overcome that challenge. Discussions and check-ins with your payments and security solution provider can help you stay on top of today's data threats and how to stop them, so you can focus on growing your business.

For more information on how Bank of America Merchant Services can help you optimize your business and customer experience, call your Bank of America Merchant Services business consultant or 855.833.3614. We're here to help.

Methodology

Unless otherwise specified, all data referenced in this report is Bank of America Merchant Services' aggregated merchant processing data and includes only card-based forms of payment. The analysis includes client settlement data from more than 539,000 U.S. merchant locations. This data reflects comparative merchant sales for periods spanning April 2016 to March 2018. (Each figure presented in this publication specifies the data range and data source studied.) These locations include small businesses, mid-sized businesses and large/commercial businesses, and the report covers both brick-and-mortar and eCommerce transactions.

Bank of America Merchant Services SpendTalk report does not indicate nor represent Bank of America Merchant Services' financial performance.

SpendTalk is provided for your convenience and information only. Bank of America Merchant Services assumes no liability for loss or damage as a result of your reliance on information in this publication. Our goal is for the content within this publication to be accurate as of the date this issue was printed. We do not guarantee the accuracy or completeness of the information presented.

About Bank of America Merchant Services

Bank of America Merchant Services connects businesses and their customers by doing payments better. The company delivers payments, eCommerce and security solutions, as well as consultation services, to businesses throughout the United States, Canada and Europe. It processed more than 16.6 billion transactions at approximately 539,000 merchant locations in 2017.[10] The company is a joint venture that combines the technology and innovative products of First Data with the relationship strength and prominent global brand of Bank of America. To learn more, please visit merch.bankofamerica.com.

---

[1] PwC's Strategy & 2017 Retail Trends https://www.strategyand.pwc.com/trend/2017-retail-trends

[2] Baymard Institute, "ECommerce Search Usability: Report and Benchmark," 2014. http://baymard.com/blog/ecommerce-search-report-and-benchmark

[3] Smart Insights, "Ecommerce Conversation Rates," April 25, 2016. https://www.smartinsights.com/eCommerce/eCommerce-analytics/eCommerce-conversion-rates

[4] Based on Bank of America Merchant Services' 2018 customer settlement data.

[5] KPMG Consumer Loss Barometer, 2016

[6] Ponemon Institute, 2017 Cost of Data Breach Study, https://www.ibm.com/security/data-breach, June 2017

[7] Javelin, "2017 Identity Fraud: Securing the Connected Life," 2017. https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

[8] Juniper Research, "Online Payment Fraud: Emerging Threats, Key Vertical Strategies & Market Forecasts 2017-2022," 2017. https://www.juniperresearch.com/press/press-releases/retailers-to-lose-$71-bn-in-card-not-present-fraud

[9] FICO, "Fico Reports a 70 Percent Rise in Debit Cards Compromised at U.S. ATMs and Merchants in 2016," 2017.

[10] Based on bankcard, other credit, and PIN debit sales volume and transactions. Per the Nilson Report, March 2018, Issue 1127.

Merchant Services

BA9419-LC-BB-CBB-BAMS-SpendTalk-ARJVYRK9-05/2018