Security Implications for Merchants—Emergence of New Payment Methods and their Fraud and Risk Prevention Considerations

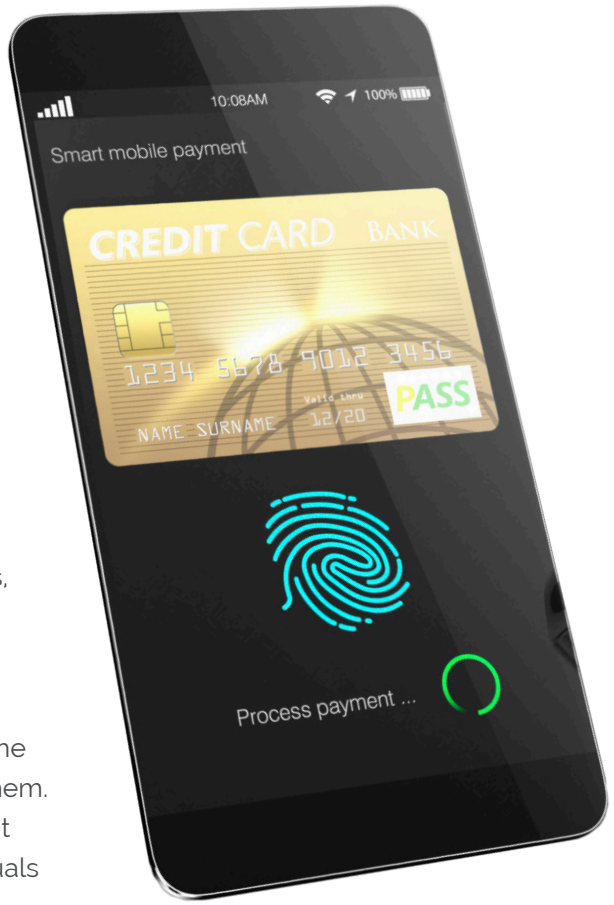
VERIFI™

The way we pay for things has changed dramatically over the years. The use of credit cards was a major shift for consumers who were accustomed to carrying around sometimes large amounts of cash everywhere they went. Today, many people don't walk around with any cash on them at all. So prevalent are credit and debit cards and electronic transactions that people only seek out an ATM in special circumstances.

So prevalent are credit and debit cards and electronic transactions that people only seek out an ATM in special circumstances.

As technology advances, a consumer's need for plastic might also begin to fade.

We're not there yet, but the emergence of new payment methods—particularly mobile payments through smartphones, smart watches, etc.—has ushered in an exciting time for the payments industry and the consumers who drive the success of their business.



There's a yin to every yang, however, and with added speed and convenience comes additional risks and security concerns for merchants, issuers and cardholders alike. In any industry, fledgling technology brings a new world of the unknown. That is, until something has been tested in the wild and some of the bugs are squashed, there will always be opportunities for people looking to take advantage of unforeseen flaws. Many times developers of new technology don't know what they don't know. It's a matter of seeing their products, systems, etc., in real-world action before they can have a full understanding of potential problems.

The rapid advancement of mobile technology and CNP systems means the good guys are always in a race to patch holes before the bad guys find them. Data security and privacy are paramount, and it's a continuing game of cat and mouse between merchants, issuers and acquiring banks and individuals seeking to commit fraud.

This paper examines some of the newer ways consumers are paying for goods and services and the security concerns that go along with them. It will also shine some light on the best ways for merchants to accommodate the new payment streams while keeping their customers' information secure and their own exposure to fraud at a minimum.

Mobile Payments and the Waning Fear Factor

Chances are, someone you know (usually a parent or grandparent) is still hesitant to make a purchase online. While these traditionalists are in the minority today, it wasn't that long ago when the thought of entering your credit card number into a website—let alone linking it to merchants for automatic withdrawal—was absolutely terrifying.

Today, we're quicker to accept and adapt to new ways of doing things, especially if the new ways are easier, which is what technology is supposed to do—make our lives easier. What's happening is a case of simplifying what the consumer must carry with them. Companies are taking everything that used to clutter your purse or wallet and putting it all in your phone. The idea is simple; the easier it is for you to pay for something, the easier it makes your decision to buy something. There has to be a benefit, and convenience is the primary focus.

"The challenge to adoption is that the vast majority of consumers don't wake up in the morning thinking 'I want to find a new way to pay today,'" Aite Group research director Julie Conroy said. "Payments are a derived demand, people pay because they want to buy something, and the majority won't change an entrenched behavior unless there's a compelling reason to do so."

It has been a slow adoption, people aren't wholesale abandoning the physical credit card swipe, but the trend to contactless payments is certainly on an upward trajectory. An eMarketer report[1], showed that while only 23.2 million people in the U.S. made a mobile proximity payment in 2015 (e.g. holding your phone near a sensor in the card reader or scanning a barcode on your phone that contains your payment information), that number is expected to rise to 69.8 million in 2019.

Further, those people, on average, are expected to spend $3,017.02 each through mobile proximity payments in 2019. That's well up from just $375.82 in 2015. That's a significant jump indicating consumers are no longer apprehensive of making payments in new ways, especially when convenience is involved.

The Aite Group predicts that mobile proximity payments will account for $487 billion in 2020[2]. It's a shift that isn't just about Joe or Jane Millennial waving around their phones to buy an energy drink at the local pharmacy. This kind of change requires merchants to have the right tools and systems in place or risk damaging their relationship with customers and irreversibly hurting their brand.

Mobile Device Payments and Beyond

The new payment method currently getting the most attention is through mobile devices. Apple Pay, Android Pay and Samsung Pay are just a few. These work with what's known as NFC (Near Field Communication) or Magnetic Secure Transmission (MST) systems that allow consumers to hold their device (whether that's a phone or wearable) near the reader at the point of sale to complete the transaction. Generally, a credit card is linked to these services and allows the buyer to forego producing the physical card at the register.

Many merchants also offer a mobile wallet within their smartphone applications that link to the cardholder's payment information and allows for payment scanned from a barcode or QR code within their particular app.

Alternative payment companies are also on the cutting edge of this shift in how we buy goods and services (think PayPal, Skrill, etc.). These providers are predominantly focused on online purchases, but they have advanced in the same fashion as individual merchant mobile wallets to allow for in-store transactions.

Bitcoin has also gained popularity. Though defined as a digital currency that bypasses banks altogether, many experts believe it might be better classified as a new payment method than an actual independent currency[3]. Bitcoin certainly complicates matters for merchants as well, due to the aforementioned fact that there is no bank controlling the flow.

Regardless of the method, all of these new forms of payment require authentication through password or pass code, or through biometrics such as fingerprint scanning.

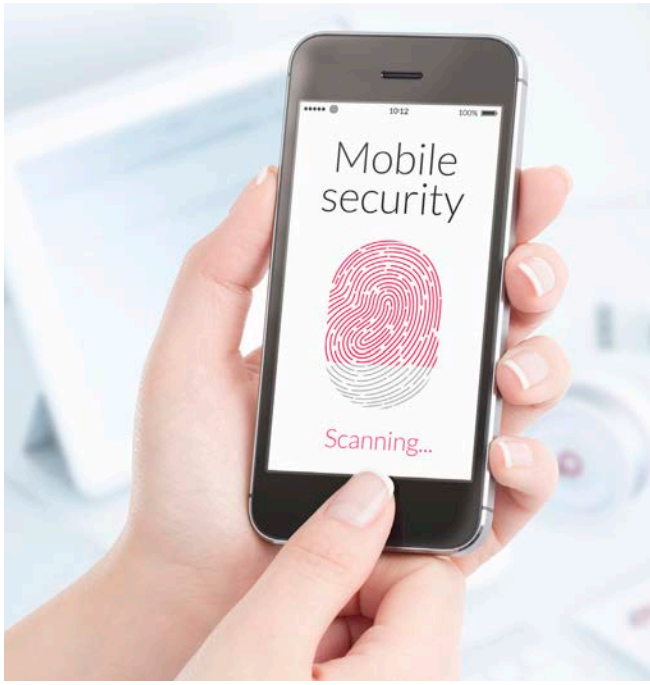
Biometrics, in fact, are picking up steam, and many developers are working on facial recognition and beyond to further authenticate the validity of payments. Most smartphones and digital wallet programs can link to fingerprints currently, which provides the consumer with the convenience of not entering a password during the transaction. The work in the space now has turned to biometric authentication that doesn't require any device to be present. That is, some form of facial or voice recognition, or a fingerprint scanner at the point of sale that is linked to a credit or debit card could be in our future.

What are the Security Concerns and Risks for Cardholders?

For consumers, the idea of leaving their credit or debit cards at home is intriguing. It can feel safer, and it may in fact be through tokenization processes that don't allow the actual card number to be relayed during the transaction[4], but according to a recent study[5] released by the global cybersecurity association ISACA, 47 percent of the experts surveyed do not believe mobile payments are secure, and 30 percent are unsure. What's more, 87 percent believe we'll see an uptick in mobile payment data breaches in the next 12 months.

There are a number of reasons for this less-than-confident feeling, the most agreed upon being the use of public Wi-Fi. Although the Internet is not required for contactless payment, there is the vulnerability of a person's information being stolen at the local coffee shop, etc. Other concerns include weak passwords, phishing attacks and lost or stolen devices.

Apart from mobile payments, alternative payment sources can be vulnerable as well. A consumer's payment information stored with alternative providers like PayPal is only as safe as the company's security system. Because Bitcoin operates in a highly uncontrolled environment, the security depends on an individual user's ability to keep their passkey(s) private[6], an endeavor that comes with its share of susceptibilities.

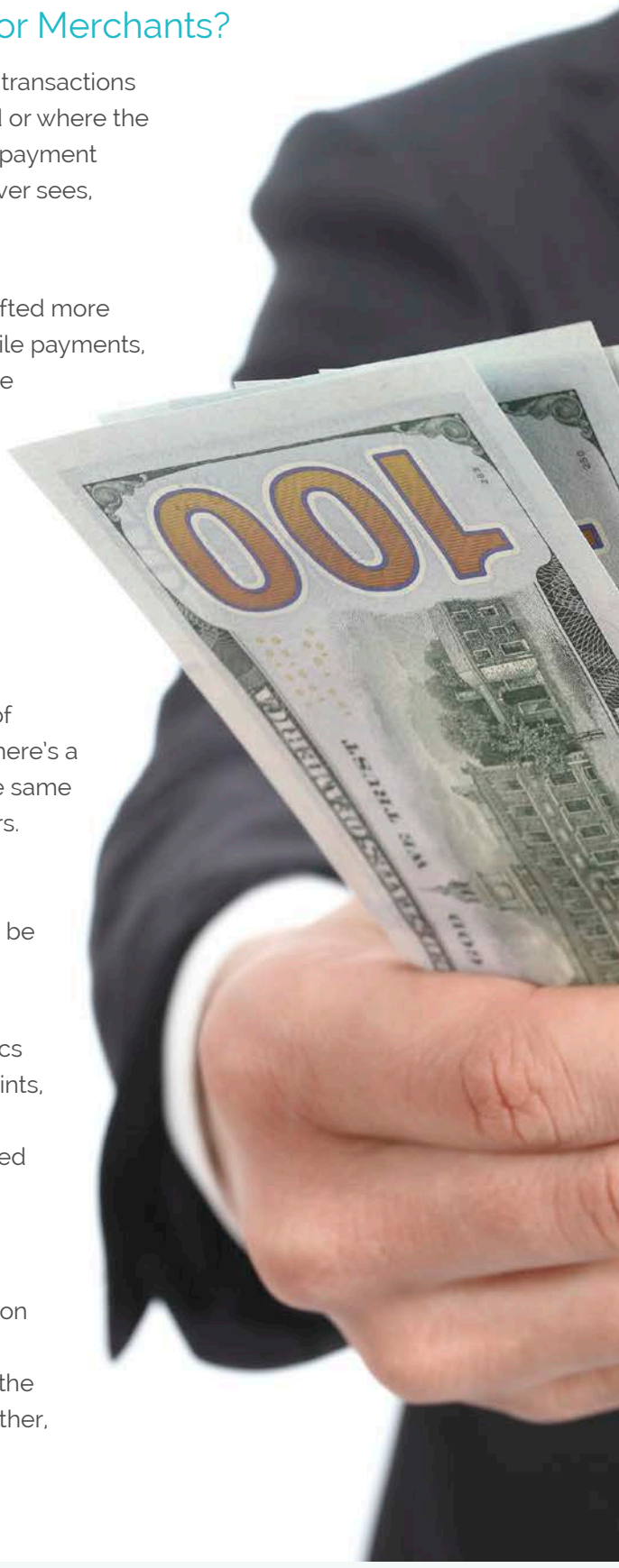


47% of the experts surveyed do not believe mobile payments are secure

87% believe we'll see an uptick in mobile payment data breaches in the next 12 months

What are the Security Concerns and Risks for Merchants?

A great deal of faith is put on merchants by cardholders that their transactions are secure at the point of sale, regardless of the payment method or where the transaction takes place. Merchants must be diligent in protecting payment information on the back end through processes the consumer never sees, and they must stay ahead of the changing tides of fraud.



For example, the emergence of EMV (chip-and-PIN) cards has shifted more fraudulent activity to the card-not-present arena. In terms of mobile payments, a LexisNexis report stated that unprepared merchants are not able to properly detect unauthorized transactions, and they risk the interception of confidential information[7]. Other mobile payment risks for merchants include the inability to track purchases without the actual credit card number stored in their system, stolen payment tokens in motion and at rest, and antiquated PoS and network systems vulnerable to attacks[8].

Acceptance of digital currency such as Bitcoin also has its share of security risks. These currencies are decentralized, which means there's a greater susceptibility to cyberattacks because they don't have the same protection traditional currencies have through payment processors. The greater exposure to cyberattacks makes it very difficult for merchants to fully protect consumers and their information. Additionally, from a practical business perspective, there can also be some difficulty in converting digital currency into legal tender.

Even the security measures can be compromised. While biometrics greatly help reduce instances of unauthorized payments, fingerprints, for example, can and have been stolen from a person's device. Likewise, tokenization system vaults are increasingly being targeted by cybercriminals, and it's a constant race to keep them out.

Inadequately protecting themselves from a growing number of security risks can result in catastrophic losses from fraud, reputation damage and chargebacks for merchants. According to a 2016 LexisNexis report, the cost of fraud has grown four times more in the mobile channel than the physical POS channel since last year. Further, every $100 of mobile fraud costs merchants up to $363[9].

How Can Merchants Reduce their Risk?

All of these risks can generate many significant problems for merchants who aren't ready for today's technological shift. Any of these vulnerabilities can open the door for increased fraud and a storm of chargebacks which can have a staggering effect.

Verifi Vice President of Business Development Chris Marchand says the adoption of newer methods of payment, especially in the beginning, could be rocky from the merchant's perspective, and it's paramount to invest in supporting systems that protect the merchant throughout the entire transaction.

"There may be some bumps in the beginning since merchants might have little or no experience with the new method of payment," Marchand said. "They should definitely understand the chargeback rules and procedures with the new methods so they understand their options and react appropriately."

New payment methods don't necessarily have the data support behind them to help merchants assess their chargeback risks very effectively.

"It will be something merchants need to watch as they have no prior history in this area of new payment methods," Marchand said. "If they don't integrate the new method into their current process and keep things similar, the consumer will have a different checkout experience and it could potentially increase the chargebacks."

Many merchants are seeing the value in solutions—like Verifi's Cardholder Dispute Resolution Network (CDRN)—that redirect a cardholder's dispute back to the merchant (and away from the issuer) to allow for a much more seamless dispute resolution process, thus, helping prevent fraud and chargebacks.

The addition of increasingly popular new payment methods is a good time for merchants to revisit their checkout protocols and make sure they are able to acquire as much information as possible about the sale. Marchand says this can go a long way should the transaction end up in the chargeback pipeline.

"It's important that the checkout process grabs all the necessary pieces of information from the consumer or will provide documentation throughout the process to set your organization up to build a successful representment if a chargeback is received," Marchand said.

Another potential trouble spot for merchants is through confusing billing descriptors that show up on a cardholder's credit card statement. New payment methods might list a charge differently than the way traditional methods have in the past, which can certainly have a negative affect on chargeback rates.

For example, some mobile wallet providers might be listed as the Merchant of Record (MoR) on a billing statement rather than the actual merchant. Adding to the confusion, these mobile wallet providers might combine several transactions into a single line item, which further reduces transparency of the charge and makes it difficult to properly track fraudulent activity[10].

A confusing billing descriptor is one of the most prevalent reasons chargebacks occur, but the confusion can be reduced through platforms that allow the merchant to share details about the transaction and validate the sale (or raise red flags for a possible breach or fraud attempt). This kind of platform gives the issuer handling the dispute call greater insight about the transaction, including details of the payment method (device used), the person who made the purchase, details of the item or service purchased, etc. Without this information, the issuer, in an attempt to keep the cardholder happy, is often faced with no other option than to administer a chargeback. These platforms aim to provide solid footing for merchants to avoid costly chargebacks and representment processes.

"There's no silver bullet," Marchand said. "Chargebacks will happen, but they can be significantly reduced, and the best defense is being prepared to deal with them on all levels."

Conclusion

New payment methods make things faster and easier for consumers, but they also add yet another layer of complexity for merchants who are responsible for securing the transaction data from start to finish. Merchants who resist these new ways to pay will be left in the dust, so it's imperative they get their systems up to snuff and integrate with solutions that can help ensure a smooth process throughout the transaction while guarding against data attacks and fraudulent activity. Mobile payment processing and other newer payment channels require greater diligence in validating the sale and preventing chargebacks, and partnering with providers who can help stop disputes before they become chargebacks and aid in winning the disputes that make it into the chargeback process.

About Verifi

From startups to Fortune 500 companies, Verifi is equipped with the versatility to work with a wide range of industries to maximize revenues and reduce all aspects of chargeback losses. Headquartered in Los Angeles, California, Verifi processes more than $20 billion transactions each year and manages more than 12,000 accounts worldwide. With its proven team of experts and award-winning custom solutions, the Verifi Difference consistently protects merchants' payments and significantly boosts profits for the entire transaction ecosystem.

VERIFI

Why Choose Verifi?

Partner with Verifi to reduce your payments risks, streamline business processes and lower operational costs. Whether it's stopping fraud, maximizing your billings on our flexible and robust global gateway or our award-winning chargeback prevention and dispute management services, our team of experts and custom solutions will protect your payments and boost your profits across the entire transaction lifecycle.

Contact Verifi

323.655.5789
info@Verifi.com
www.Verifi.com

Citations

1. http://www.emarketer.com/Article/Mobile-Payments-Will-Triple-US-2016/1013147
2 http://aitegroup.com/report/mobile-proximity-payments-disruption-force
3 http://insidebitcoins.com/news/payment-expert-says-bitcoin-has-more-potential-as-a-new-payment-system-than-a-currency/25966
4 http://www.isaca.org/cyber/cyber-security-articles/Pages/mobile-payments-more-secure-than-conventional-payments.aspx
5 http://www.isaca.org/SiteCollectionDocuments/2015-Mobile-Payment-Security-Study-Global-Data-Sheet_mis_Eng_0915.pdf
6 http://www.tripwire.com/state-of-security/security-data-protection/security-issues-may-chronically-hinder-bitcoin-adoption/
7 https://www.lexisnexis.com/risk/intl/en/resources/whitepaper/Understanding-The-New-Payment-Methods-CSMB.pdf
8 http://www.isaca.org/cyber/cyber-security-articles/Pages/mobile-payments-more-secure-than-conventional-payments.aspx
9 http://www.lexisnexis.com/risk/insights/true-cost-fraud.aspx
10 http://www.aba.com/Tools/Function/Payments/documents/2013EmergingPayments.pdf