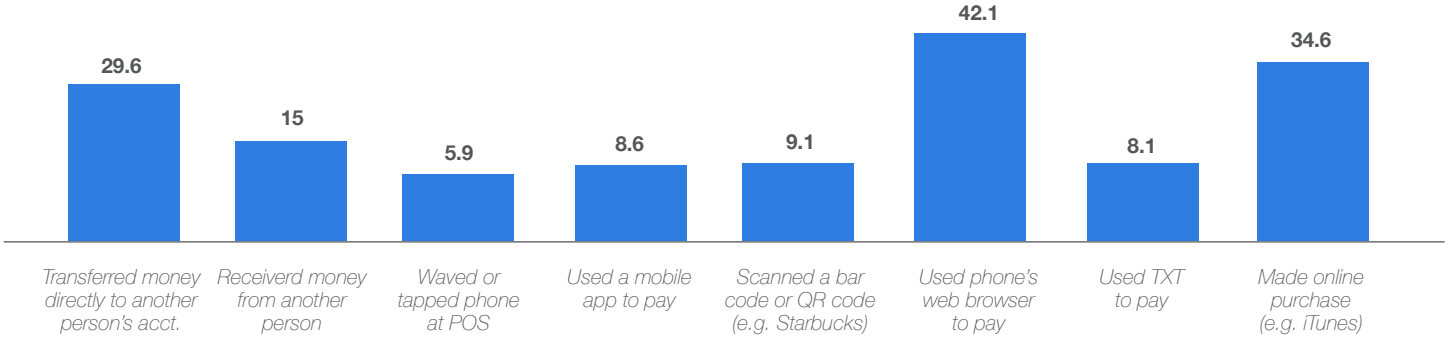
VERIFI™

What Every Merchant Needs to Know About Mobile

VERIFI WHITEPAPER

What Every Merchant Needs to Know About Mobile

Increased consumer interest in mobile payments, the emergence and integration of Apple Pay and the shift to EMV will result in an enormous surge in mobile payments during 2015 - including both the emulation of an online purchase via a smartphone/ tablet and the use of smartphones to make a purchase in a brick-and-mortar environment (mobile proximity). The latter is not yet a commonplace occurrence – according to the 2013 Federal Reserve "Consumers and Mobile Financial Services" report, only 25.6% of consumers who have used mobile to make a payment of any kind had made a mobile proximity payment. This year, there are influencing factors that will affect change in mobile proximity payments: near-field communications (NFC) and EMV.



Source: Federal Reserve: Consumers and Mobile Financial Services 2013

Mobile payments poses unique challenges when it comes to fraud prevention, conversion optimization, cart abandonment and streamlining payments. This white paper outlines what to expect in 2015 as well as ways to optimize – and protect – these payment type from increased risk and fraud.

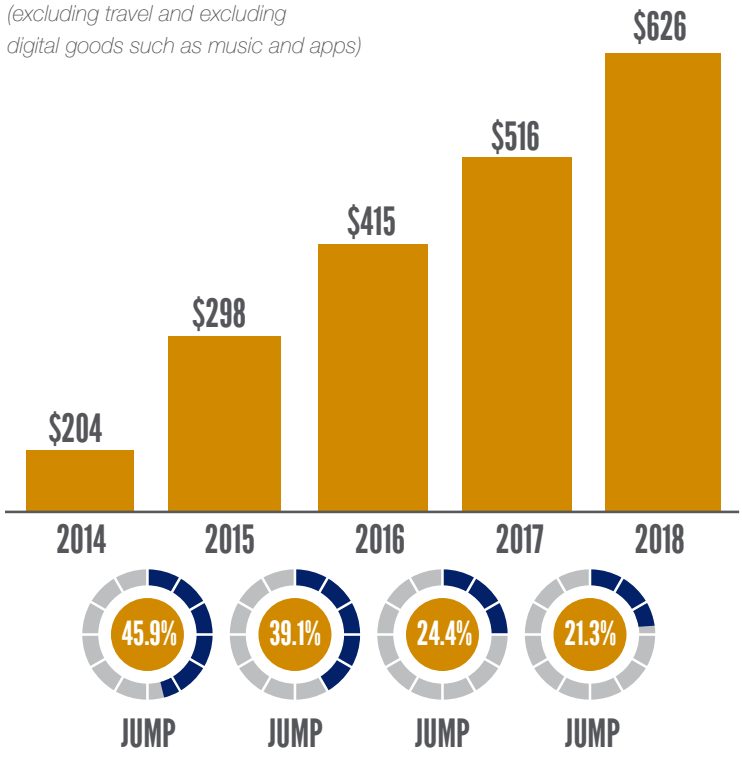
The State of Mobile Commerce

2015 appears to be the breakout year for mobile payments. Retailers are quickly integrating mobile into the overall retail shopping experience, resulting in more sales opportunities both on-device and in-store. Goldman Sachs predicts that mobile commerce will account for almost half of all e-commerce by 2018, with tablets increasing in popularity and causing a jump in spending to $626 billion in 2018. In addition, it's estimated that 525 million worldwide consumers will purchase via mobile this year[1] with global B2C commerce sales forecasted to top $1.7 trillion and mobile commerce contributing roughly $300 billion in sales.[2]

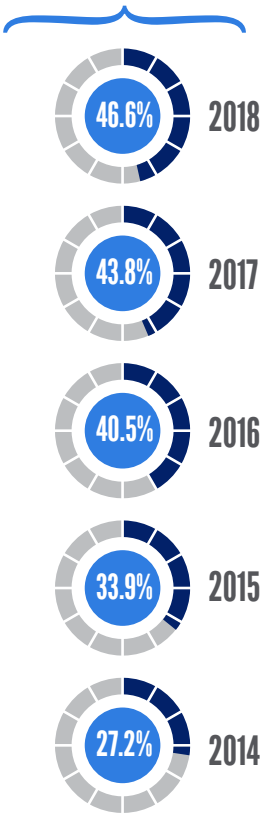
Goldman Sachs Predictions[3]

Retail Mobile Commerce Sales

(excluding travel and excluding digital goods such as music and apps)



Percentage of Mobile Commerce that will Represent of E-Commerce Sales



For those merchants poised to properly harness the power of the channel, windfalls can be huge…but this does not come without added risks. As we saw during last year's holiday season, there are potential obstacles and gaffes that can occur if merchants are not prepared. Merchants who have not yet tested the mobile waters (and even those that have) should tread carefully and not rush into expanding without establishing the proper groundwork. Best Buy is illustrative of one issue this past Black Friday.[4] Due to overwhelming – and unexpected – amounts of mobile traffic, the Best Buy website had to be shut down for an hour on Black Friday. That is not an ideal situation at anytime, let alone during a peak-selling day. Yet this is not a rare occurrence – many retailers do not have mobile optimized sites and the average mobile site takes seven seconds to load.[5]

Balancing Convenience and Security

Merchants face a unique and constant battle: providing the best purchasing experienced with its customers while maintaining a fluid and appropriate fraud management strategy. As mobile commerce adoption becomes more mainstream, consumers have increased expectations for ease-of-use, personalization of experience and convenience. Merchants need to provide a streamlined experience without sacrificing safety and security, though finding that balance can be difficult. There are a number of ways that merchants can optimize user experience, reduce cart abandonment and still provide a secure transaction experience that extends throughout the transaction lifecycle.

OPTIMIZING USER EXPERIENCE – CONVERSION OPTIMIZATION

Responsive design is key. Shoppers are increasingly turning to mobile – both smartphones and tablets – to make a purchase and merchants should leverage responsive design to optimize user experience. Consumers expect a seamless shopping experience across devices, screen size and operating system and this type of unified branding can boost site conversions.

Additionally, utilizing customer data can allow online merchants to engage consumers with sophisticated targeting, personalization and promotions on mobile.

CART ABANDONMENT – STREAMLINING CHECKOUT EXPERIENCE

User experience allows the consumer to access and use your site easily, but making a payment is another story. Experts estimate that the mobile cart abandonment rate is close to an astounding 97%.[6] Logging in and entering payment information can be burdensome for shoppers on a smartphone. Small screens and keyboards can pose obstacles when a lot of information and clicking is involved. Merchants can simplify the checkout process by reducing the amount of information required to checkout. This can be accomplished by saving payment information, enabling one-click purchasing or allowing customers to use social logins to complete a purchase.[7]

Merchants have tools to combat this exceptionally high cart abandonment rate, including retargeting and sending post-cart abandonment emails with discounts. A/B testing software company vwo.com's research shows that over 55% of online shoppers would consider purchasing an abandoned product if offered a discount on it after the fact.[8]

SECURITY CONCERNS – SOPHISTICATED FRAUD PREVENTION

This is a pivotal topic in mobile and one that will continue to evolve as NFC takes hold in the marketplace risks shift toward the card not present environment when EMV is rolled out this year. According to a study by LexisNexis and Javelin Strategy & Research, many small mobile merchants use less fraud-prevention tools, opening them up to more fraud. These smaller merchants average just two types of fraud solutions whereas larger merchants are employing an average of four types. These fraud tools include PIN and signature authentication, transaction and customer profile databases, and IP geolocation among others.[9]

That same study pointed out that mobile fraud is almost three times as expensive as the actual cost of the stolen good, due to fraud investigation, chargeback fees and payment processing costs.[10] Given this, merchants should be stepping up fraud prevention by layering tools that can work together to provide a safe, frictionless purchasing experience for shoppers while stopping fraudsters in their tracks.

Mobile payments have their own set of issues and require tools tailored to bridge its unique vulnerability gaps from beginning to end. We've outlined some of the most-used mobile fraud prevention tools in the table below:

Tool	What it does	How it works	Downside to using it alone
Device Fingerprinting	Device fingerprinting enables merchants to recognize a particular device that has been used to make a previous purchase as either a device that was used before to conduct successful transactions or was used to conduct fraud online.[11]	Some systems use browser environment fingerprinting while others use techniques to uncover characteristics about the actual machine hardware. Emerging technology includes cryptographically strong versions of device identification systems that will help identify fraudsters who attempt to make their machine appear different every time they commit fraud.	Fraudsters can circumvent this tool through virtual private network (VPN) or proxy services that hide the device's IP address. Cyber criminals can also disguise sessions from a single computer to make it seem like they are originating from a number of different computers, browsers and operating systems.[12] Merchants should employ device fingerprinting as one component of a comprehensive, layered security solution.
Geolocation	Geolocation data can confirm the location of a customer and use the information as part of the transaction fraud scoring and authorization decision for mobile transactions.	Geolocation reports your location to other users, whether you're on a desktop or a mobile device. Smartphones include a GPS chip that uses satellite data to calculate your exact position. If a GPS signal is unavailable, geolocation uses information from cell towers to triangulate an approximate position.	Merchants can use geolocation to verify that the location of a mobile device is the same as the place of a purchase (at a brick-and-mortar location). When it comes to CNP transactions, geolocation becomes trickier because mobile users are on the move and the location of the device is always changing. This can raise issues for fraud detection software that can't get a read on whether the purchase should be flagged as suspicious.[13]
IP Intelligence	IP address sourced geo-location and proxy-piercing information, provides in depth, non-invasive insight into the risks involved with accepting transactions from specific IP addresses.	IP intelligence solutions provide accurate and reliable IP data to identify suspicious activity to help companies determine whether additional verification is required, deny a request or invalidate a click for all online transactions based on workflow rules.	This tool works best when used with mobile geolocation and device fingerprinting as one characteristic (either IP address, location or device ID) is no longer enough to effectively categorize a purchase as suspicious or not. Fraudsters have found ways to exploit these identifiers separately, so it's in a merchant's best interest to validate all three for the most accurate read.
Pre-Chargeback Notifications	Immediate notification of cardholder disputes from the card Issuers helps stop the fraudulent shipments of orders before they become a loss and gives the merchant an opportunity to respond to the dispute and resolve the issue before it becomes a chargeback.	Issuer/merchant collaboration in addressing the issue facilitates a quick and easy resolution: processing a refund or issuing a credit, ultimately preventing the chargeback, supporting good customer service and provides valuable back end information which can point to issues in the business operations.	Merchants should not rely on pre-chargeback notifications alone as front-end fraud prevention tools are necessary to maintain an acceptable chargeback ratio. Augmenting fraud prevention tools with pre-chargeback notifications allows merchants to dial back front-end fraud prevention tools, decreasing false positives while respecting the limits of the risk threshold.

Outsourcing fraud management can be a valuable consideration for merchants who cannot dedicate the proper resources to protecting payments.

Whether managing mobile fraud prevention in-house or utilizing the specialized expertise of a third-party vendor, merchants should remember that a comprehensive strategy and solution cannot be taken lightly or ignored. Merchants that manage fraud in-house often have customer service track and verify transactions and IT handle solution implementation. Effective in-house fraud prevention should lean on IT for the majority of fraud prevention needs so they can use information about mobile – and all – transactions to properly toggle fraud prevention tools and protocol. The problem with this approach is that it requires an abundance of readily available IT resources – a scarcity for most merchants.

Employing the help of an outside vendor can save time, money and resources – as well as reduce the burden on an already stretched-thin IT department. One size does not fit all when it comes to fraud prevention and as mobile adoption increases, new vulnerabilities will likely come to light, requiring an even greater level of attention paid to this channel. Outsourcing fraud management can be a valuable consideration for merchants who cannot dedicate the proper resources to protecting payments.

How Verifi can help

Verifi helps merchants consistently stay one step ahead of sophisticated fraudsters by providing a comprehensive fraud management platform that enables merchants to layer, test and adapt this suite of best-of-breed tools as the marketplace – and fraudsters – evolve. The Intelligence Suite® is a cost-effective way for merchants to safeguard their card-not-present (CNP) transactions across multiple channels without cumbersome, expensive IT involvement and numerous costly integrations or reintegrations.

As illustrated, using disconnected, one-dimensional or piecemealed solutions leave merchants vulnerable. Intelligence Suite closes the security gap by providing a personalized technology hub that allows for the rapid integration and fine-tuning of fraud controls. This fraud prevention platform combines tools that touch all critical fraud prevention verification points, including consumer, device, mobile, IP geo location, and payments channels – all through one easy integration. Verifi's proprietary rules engine makes it easy to customize how to best use these tools and to what degree, enabling merchants to test and toggle combination on the fly to stop emerging threats. THE RESULT - broad fraud protection without hindering conversions; the ability to customize allows merchants to let more successful and legitimate sales pass through without increased risk.

When combined with our award winning, Cardholder Dispute Resolution Network™ (CDRN), merchants can take fraud prevention one step further by minimizing fraud loss without inhibiting sales on the front end. Pre chargeback notifications help merchants ease front-end fraud screening to boost sales while reducing chargeback rates and lowering overall fraud costs. This forward-thinking combination of solutions allows merchants the latitude to provide a secure experience to consumers while allowing for adjustments in response emerging threats, emerging technology and new sales opportunities as the card-present and card-not-present environments continue to blend.

Mobile Blurs Card-Present and Card-Not-Present Channels

Mobile transactions are classified as card-not-present (CNP) transactions, but that line has begun – and will continue – to blur as mobile transactions become as, or more, secure than card-present transactions. Eventually, this may lead to a change in their interchange treatment.

Mobile transactions are classified as card-not-present (CNP) transactions, but that line has begun – and will continue – to blur as mobile transactions become as, or more, secure than card-present transactions.

The biggest drivers of change in mobile for 2015 will be the use of NFC as the de facto method to make mobile payments as well as EMV and its impact on merchant terminals. Merchants are in the process of installing terminals to enable EMV and a majority of these are NFC-capable. The Aite Group points out that most merchant terminals will be able to accept NFC transactions in the next one to three years.[14]

EMV, NFC AND IMPLICATIONS

As the U.S. inches toward full implementation of the EMV standard, merchants can expect a subsequent migration to a "contactless world". A large reason that so many retailers are already NFC-capable (and most will be by the end of this year) is because of EMV. The majority of large retailers carry NFC-capable registers and about 6 million NFC-compatible store registers shipped last year alone.[15] The terminals merchants are installing for the EMV migrations are also NFC-capable, so merchants that haven't quite adopted NFC in their stores yet, will in the next one to three years.[16]

The security features of NFC rival that of card-present transactions – if not exceed them – and this trend will lead to a blurring of the two channels. Apple Pay encrypts payment card data and authentication occurs with Touch ID, a type of biometric tool. This system is highly secure and exceeds security of mag-stripe cards, which are easily skimmed, cloned and stolen.[17]

With almost all smartphones NFC-enabled (roughly 90% of global smartphone shipments will carry NFC moving forward[18]), a ubiquitous method has been created for exchanging information between mobile device and POS terminal.

A Look Ahead

While mobile is gaining momentum, there is still some fragmentation hindering widespread adoption near term. While consumer behavior may change in the interim, one thing remains certain: Merchants moving into this channel need to focus on providing a non-clunky and safe experience for consumers.

As the lines between channels continue to blur with mobile, security will be top-of-mind with both interchange and consumers. While mobile payments are headed in the direction of security that overshadows traditional card-present transactions, consumers are not necessarily buying it. Many shoppers are still not educated about the security of mobile transactions and remain uneasy about breaches and hackers.

Mobile commerce has unique vulnerabilities and merchants should ensure they are using the right combination of tools that address this channel's nuances. Given the rapid pace in which mobile channel adoption is expanding, CNP merchants who fail to dedicate proper attention to adapting the right tools to their business may experience detrimental impacts to their bottom line in the very near future.

About Verifi

Verifi, an award-winning provider of end-to-end payment protection and management solutions, was founded in 2005 to help our clients effectively manage the payments challenges they face everyday. Verifi helps merchants safely process payments, combat fraud, prevent and resolve costly chargebacks, as well as increase billings and keep loyal customers. Our best-in-breed solutions and white glove support are trusted by a wide range of industries from emerging companies to the Fortune 500. Headquartered in Los Angeles, California, we process more than $20 billion transactions annually and currently serve more than 5500 accounts internationally.

VERIFI™

For More Information

Main Phone: (323) 655-5789 Mon-Fri 8:00 AM – 5:00 PM PST

Main Fax: (323) 655-5537

Email Address: info@verifi.com

Mailing Address: 8391 Beverly Blvd., Box #310, Los Angeles, CA 90048

Citations

1 *https://www.internetretailer.com/2014/03/10/mobile-commerce-will-be-nearly-half-e-commerce-2018*

2 *http://www.cio.com/article/2866080/e-commerce/how-ecommerce-businesses-can-beat-the-competition-in-2015.html*

3 *https://www.internetretailer.com/2014/03/10/mobile-commerce-will-be-nearly-half-e-commerce-2018*

4 *http://fortune.com/2014/11/28/best-buys-website-down/*

5 *http://www.businessinsider.com/e-commerce-mobile-and-web-benchmarks-2015-1#ixzz3O9Su53ml*

6 *http://www.optaros.com/insights/blog/abandoned-shopping-carts-are-running-rampant-mobile-commerce-what-you-can-do-about-it*

7 *http://www.cio.com/article/2866080/e-commerce/how-ecommerce-businesses-can-beat-the-competition-in-2015.html*

8 *http://www.cio.com/article/2866080/e-commerce/how-ecommerce-businesses-can-beat-the-competition-in-2015.html*

9 *http://www.businessnewsdaily.com/5884-mobile-payments-increase-fraud-risk.html*

10 *https://www.calbanktrust.com/blog/3-simple-steps-to-fight-payments-fraud*

11 *http://www.darkreading.com/risk/the-value-of-device-authentication/d/d-id/1137005?*

12 *http://securityintelligence.com/how-fraudsters-are-disguising-pcs-to-fool-device-fingerprinting/#.VL_1PktgYds*

13 *http://www.merchantaccountguide.com/merchant-account-news/in-rush-to-mobile-market-merchants-vulnerable-to-fraud-28.php*

14 *20150113-Top-10-Trends-in-RB-2015-NOTE-pdf_6713_18213_10125_10860.pdf*

15 *http://www.businessinsider.com/what-you-need-to-know-about-apples-new-payments-system-2014-9#ixzz3O9S5mZ7K*

16 *20150113-Top-10-Trends-in-RB-2015-NOTE-pdf_6713_18213_10125_10860.pdf*

17 *http://www.businessinsider.com/what-you-need-to-know-about-apples-new-payments-system-2014-9#ixzz3O9S5mZ7K*

18 *http://www.businessinsider.com/what-you-need-to-know-about-apples-new-payments-system-2014-9#ixzz3O9S5mZ7K*