The Risks Of Mobile Wallets

cyber security payments risk management

Summary: Mobile wallet technology is becoming increasingly popular. But, just like any technology rapidly on the rise, there are growing risks to consider.

In the past decade there have been some ongoing and significant changes in the banking industry. One of those surfaces by JD Power which finds that while mobile banking customer adoption was low in 2009, it has grown so much that 53% of retail banking customers now say they use mobile banking in 2019. Also over that time, the Fed reports the number of commercial bank and thrift branches has declined nearly 10%, or just over 1% per year. A changing environment these days is expected.

When looking at the industry, other changes are also happening in mobile wallets. The technology is becoming increasingly popular. But, just like any technology rapidly on the rise, there are growing risks to consider.

Mobile wallets allow users the convenience to store information from one or more credit or debit cards (encrypted as 'tokens') on their smartphone. While credit and debit cards of the plastic variety still dominate the scene, the use of mobile wallet technology for payment has been on the rise for roughly 9Ys. Research aggregator Statista forecasts global mobile payments will rocket to more than $1T by the end of this year.

So, it's little surprise that even the most cautious community bank is now at least considering supporting mobile wallet options. If you are one of them, be sure to take into account the potential risks that mobile wallets carry too (if for no other reason than to help educate customers). Potential mobile wallet risks include:

1. **Phone theft.** Most people have come to think of their smartphones as extended appendages, but they still can be misplaced or stolen. If the mobile wallet application with a customer's card details is not properly secured, preferably with two-factor authentication, losing a phone is pretty much the same as losing your credit or debit cards themselves. Fix: Encourage customers to use the available embedded security within the mobile wallets as well as within their smartphones themselves. Remind customers to protect their phone and wallet passcodes, and beware of "shoulder surfers" just as they would at an ATM.
2. **Wallet spoofing.** Within the mobile wallet application, credit or debit card numbers are securely encrypted. They are masked by a code created by an algorithm, which creates a "token" that contains the card details. In this way, mobile transactions themselves are very secure. But, if mobile users add cards to their account while they are on an unsecured public wireless network or one that has been infiltrated, a cyber-thief can easily enough re-create or "spoof" that mobile wallet's registration and create their own phony account with legitimate payment information. Fix: Advise customers to load their cards on their own secured, home Wi-Fi network or a virtual private network.
3. **Mobile malware.** Just as cyber-criminals use malware to infiltrate computer networks, so too are they increasingly creating malware that propagates on mobile devices and allows them to steal information. Fix: Here again, cardholder education and security hygiene are the best forms of protection. Warn customers to use the same cautionary steps with links as they would on their PC and be wary of unsecured sites.

HEDGING SERVICES FOR COMMUNITY BANKS

Community bankers seeing long-term fixed rate demand from business clients can transform payments into a floating rate on their books using Borrowers' Loan Protection (BLP). Contact us today for more information.