Making A Case For Added Security At The ATM Vestibule
Based On Current Trends In Retail Banking

Published on 15 Jun 2015

A retail banking tipping point is fast approaching with the state-side adoption of EMV technology

Banking faces a challenge: to reconcile major security concerns with improving technology in order to reflect modern, mobile technology and the self-service solutions that customers have come to expect from their non-banking retail experiences. This is probably the number one issue I discuss with my bank clients. Banks need to make the technology in their branches more automated, more digital, and more mobile. All while protecting their valuable infrastructure and customer security.

Increasing Bank Security
Today’s customers expect personalized solutions. The physical bank branch needs to reflect this. In all other retail operations, we are seeing a progression toward interactive, digital experiences. The same needs to happen with retail banking in order to ensure customer loyalty. “The increasing pace of digital adoption will see more innovation from large banks in their digital strategy – and simultaneously the reshaping of branch networks and front line roles to re-position physical distribution as a strategic asset,” say consultants at Accenture.

Banking security must be improved as new designs and technologies are being deployed. The world is not getting any safer. According to a European ATM Security Team (E.A.S.T) 2015 report, “financial loss from skimming is on the rise,” up 13% when compared with 2013. This rise was largely driven by an 18% rise in international skimming losses. ATM related physical attacks rose 17%. And with physical attacks, collateral damage to equipment and buildings can be quite costly.

In the Northeastern United States, skimming attacks moved from ATM Machines to unprotected ATM vestibule doors, and we are now seeing this trend spread across the country. Just this week (May 27, 2015) a woman was robbed at knifepoint in a Massachusetts ATM vestibule. Some ask, why have an ATM Vestibule at all, if it just increases vulnerability?

Unprotected ATM Vestibules

"The increasing pace of digital adoption will see more innovation from large banks in their digital strategy – and simultaneously the reshaping of branch networks and front line roles to re-position physical distribution as a strategic asset”

ATM Vestibules, or lobbies, are installed for many good reasons. For one, more convenient, 24/7 locations equals better customer retention for a bank, offering comfort and convenience. 24/7 access to ATMs, night drops, coin counters, online banking kiosks, and other self-service solutions are very much in demand (52 percent of bank consumers would like to see more interactive, digital screens in the bank). Second, ATM Vestibules protect customers from inclement weather and to provide a more comfortable banking environment (however, vagrancy
can be an issue; therefore ATM Vestibules should require card access). The ATM vestibule environment must add security with proper security and surveillance equipment. They can’t just be for show.

Walk down any major city street and you will see the majority of pedestrians are utilising their mobile devices. They talk, shop, and bank on their mobiles. In major retail establishments, mobile devices connect to an in-store network of digital signage and apps to enhance the customer experience. So too are airports moving toward mobile integration. This is referred to as an “omni-channel” experience. We know that consumers have come to expect this - along with 24/7 accessibility - in the banking environment as well.

Protecting Consumer Interests

Clearly, being customer oriented, for banks, now means installing self-service tools that are interactive and digital. My advice is to protect these improvements with the latest technology to prevent crime, such as robberies and skimming of customer identity. An overwhelming 86 percent of consumers trust their bank over all other institutions to securely manage their personal data (Accenture research 2015). The consumer is totally in the dark when it comes to the risks that come from walking into an ATM Vestibule that is not equipped with multiple surveillance cameras (doorway, ATM, 360 degree full coverage of environment to eliminate blind spots), skimmer detection, ancillary communication devices (ATM/Banking phones), and proper lighting at all times.

A retail banking tipping point is fast approaching with the state-side adoption of EMV technology, another security measure to protect customer data (EMV stands for Europay, MasterCard, and Visa; it is the global standard for integrated circuit cards, more commonly referred to as “chip” cards, which are harder to skim than a magnetic stripe). In retail, liability for data breaches is shifting from the card issuers to the merchants, with an original shift deadline of October, 2015. This is causing major upheaval for merchants, who are dealing with not only implementing new EMV technology, but who are also dealing with the onset of the busy holiday season right around the corner. Additionally, not all banks have issued EMV debit cards to date.

Once the merchant deadline has passed (critical mass will most likely occur later in 2016 – merchants are lobbying congress to push the deadline back), and consumers are used to using
“chip-and-pin” contact EMV cards instead of mag-stripe “swipe” technology, retail banking will undoubtedly follow suit. Also on the horizon, and perhaps more importantly, is mobile technology adopting near-field-communications, or NFC, which enables smart phones and other devices to establish a radio communication without physical contact. EMV chips can also be contactless. Only when bank access control and retail banking allows for NFC technology will we truly be able to offer millennial customers the personalized and secure banking they desire. Contact, “chip-and-pin” EMV will soon be obsolete, and NFC/Contactless EMV will take over.

This is an exciting time for every industry as we move forward and re-imagine customer experiences, while improving security at the same time. Millennials are taking over and replacing Boomers, and have come to expect digital and personalized solutions. Successful businesses are adapting to this trend, driving holistic loyalty programs based on multiple elements, especially customer experience and security. Self-service, automated, and personalized solutions can provide an infrastructure backbone for added security features, as well.

Author Profile

Rob Leiponis