ATM Servicing - In House Or Vendor?

risk management ATM

Summary: While some community banks still manage their own ATMs entirely, an increasing number have hired armored carrier service providers to handle this. What are the considerations for each?

People and animals can be weird, yet similar. Psychological research now finds similarities between humans and the animal kingdom in the way they approach certain ventures. It seems mice and rats (like humans), are less likely to give up and move on to something else, once they have sunk time and effort into it.

This trait of persistence serves bankers well though in protecting customers against ATM fraud. As such, we thought we would update you further here, since ATMs still play an important role as a retail delivery channel for community banks.

While some community banks still manage their own ATMs entirely, an increasing number have hired armored carrier service providers to handle service and cash management for their machines. For some banks, the choice is about efficiency and lack of internal staff. For others, it is more a question of risk mitigation and maintaining a seamless service for customers.

Whatever the rationale, here are some issues that community banks should consider in determining whether or not to manage their own ATM service and replenishment in-house:

Employee safety. The past 5Ys have witnessed a substantial rise in robbery attempts and attempted homicides at ATMs being serviced and filled. According to the 2017 US Robbery Trends report, between 2013 and 2017, 34% of robberies occurred at ATMs. By comparison, just 22% occurred at bank branches. Sadly, more than 20% of the ATM-located robberies involved attempted homicide. While your community largely dictates the degree of safety issues with ATM servicing, these are all important things to remember before assigning internal staff.

Keeping up with technology. Delivery technology and security often focus on online and mobile channels. However, the ATM is still an access point that offers both opportunity and potential risk for banks. According to the ATM Industry Association report as of May 2018, more than nine out of 10 of US ATMs are able to process an EMV chip. Yet many of the few remaining magnetic-stripe-only holdouts are community bank ATMs. Many still need to be outfitted to accept contactless EMV and mobile payments, as well as given increasingly frequent routine system upgrades. This is to say nothing of optional updates that might engage customers, like offering imaged receipts or selling stamps through the teller machine.

Maintaining proper security. It is tough to stay on top of all the security, and that includes ATM security too. The instances of ATM skimming are on the rise, as new and more complex types of attacks pop up. According to the State of Card Fraud report, ATM fraud attacks rose 10% between 2016 and 2017 alone, with ATM cashout losses over fewer than 48 hours averaging at least $150k. In September, the Secret Service also warned of a new type of attack, called ATM "wiretapping." There, crooks bore a palm-sized hole in a cash machine and then use a combination of "magnets and medical devices to siphon customer account data directly from the card reader," according to KrebsOnSecurity.

Whether handling ATMs in-house or partnering with a vendor to do so, banks need to do everything in their power to stay on top of the latest trends and prevent the ongoing variety of fraud. We hope our update helped a bit with this.

OUTSOURCED PROFITABILITY SOLUTION FOR YOU

ProfitIntel is an outsourced relationship profitability solution that combines a powerful pricing model with full-time consulting support. Contact us today for more information.