Three Branch Security Tips During COVID-19

biometrics risk management pandemic

Summary: With the ongoing pandemic, community financial institutions may find branch security more challenging. We give you three tips to conquer branch security issues.

While bears and tigers often top the list as the most dangerous animals, so do human beings. It is not surprising then that bankers need to take extra precautions these days trying to ensure bank security.

A financial institution's first retail delivery channel has always been the branch. Even though digital banking has surged lately, the branch remains in many ways the best way for bankers to connect with customers. But keeping branches secure has become a bit more challenging, with some of the effects of COVID-19, such as face coverings and physical distancing.

Here are a few tips for how CFIs can keep their branches protected and secure during the coronavirus.

Look to biometrics. Some financial institutions are not only using biometrics (like fingerprint scanning) for authentication, but also for other aspects of security. For example, identification-scanning devices, proximity sensors, and beacon technology are being used to identify customers as they enter a branch and alert branch staff to their arrival (or of any potential security issues). By tracking customers through their mobile phone's location services or RFID tags embedded in their debit cards, CFIs can improve their security and enhance the customer experience.

Use new branch designs to your benefit. Many bankers believe that emerging branch models, including open floor designs, can present opportunities to better secure the institution. While tellers or universal bankers need to be more discreet in an open concept, CFIs are also making more use of cash recyclers, which minimize the need for the less-secure traditional teller drawer. Also, smaller branches are replacing conventional large-scale vaults with modular safes, which are more cost-effective and less risky.

Check in-branch systems. While a branch is a physical retail delivery channel, the digital networks need to be secured here too. As branches increasingly embrace the use of more customer-facing and employee-use devices and access points, there are more potential entry points that intruders could exploit. For example, a branch staff member using a tablet to assist a customer or your customers using the information touchscreens or free WiFi access are all vulnerable to security issues. Your IT team should regularly verify that certain internal networks and systems are walled off from customer access and even consider isolating from the wider network any mission-critical data or operational networks.

As you open your branches up wider to customer access, there could be new security challenges. However, with some thoughtful modifications and tightened review in key areas, your branches can remain safe and secure and still welcoming to your customers.

FASTER PAYMENTS WITH CHECK IMAGING FOR CANADIAN CASH LETTERS

PCBB's enhanced cash letter service for Canadian checks can help your institution minimize its credit exposure, increase operational efficiency, and deliver faster fraud notification. Learn more about our check imaging for Canadian cash letters.