* Utilize a locksmith to change locks and keys, ensuring they are signed out and back in after being serviced.
* Any ATM technician must obtain prior approval before they arrive to service a machine and authenticate their identity before releasing keys.
* Remove or disable ports or access points where unauthorized devices could be attached internally.
* Ensure ATM hard drives are encrypted and password protected.
* Removing the hard drive should disable the ATM, requiring an ATM technician or your IT staff to reboot the system.
* Install layered alarms inside ATM doors and high-grade sensors to enhance security.
* Take all "cry wolf" alarms seriously; they may test law enforcement and financial institution response times.
* Deploy multiple cameras for overhead and outward-facing ATM surveillance.
* If you can create an alarm to notify you when a person is at the ATM for an extended period (+ 4 minutes or some time frame), and if you can remotely access the video by phone.
* Use high-quality, color cameras capable of clear nighttime recordings.
* Secure the base of free-standing ATMs with alarms and bolting mechanisms.
* Apply the same security measures to ATMs in convenience stores, hotels, casinos, and similar establishments.
* Prevent exposure of ATM cabling from the back, sides, or front to reduce vulnerabilities.
* To deter chain-based pull-off attacks, utilize pillars or metal framing around free-standing ATMs.
* Consider an internal GPS locator to aid in ATM recovery and potential apprehensions.
* Display warning signs indicate that the ATM has been upgraded with tampering prevention and enhanced recovery capabilities.

**If an attempt is made to break in, steal, or damage the ATM, report to the police for possible fingerprinting and pull all video for police investigation. Also, let FRPA know (****kate@frpafraudviewer.org****), we try to alert other Banks and Credit Unions**

**Questions call John McCullough, 612-328-3651, or email cppcfe@aol.com**