U.S. P&C Fraud Management

Fraud Alert

Incident:

Skimming devices have been recently identified on BMO Harris drive-up and vestibule ATMs. "Skimmers" are card-reading devices attached to ATMs by fraudsters in an attempt to collect our customer's card and pin data. See this Sales & Service Update for more information.

Location:

All regions are at risk– currently reported in IN, IL, MO regions

Red Flags:

Skimmers, cameras, and false pin pads may alter the appearance of the machine, and may wiggle insecurely if present. Additionally, customers may complain of frequent issues while using the machine. A skimmer that has been removed may leave behind some sticky residue. **SEE THE PHOTOS ON PAGE 2.**

Action Required:

Become familiar with the normal appearance of your ATMs and inspect them daily. Escalate any indicators of the presence of a skimmer based on the red flags above. **Do not attempt to remove skimming devices.**

Contact:

Your manager, and I&SS (hyperlinked below). **If you have inadvertently removed a skimmer from an ATM, call the local police** prior to calling I&SS.

Fraud Detection and Investigation Services (FDIS)

During the hours of 7:00 a.m. CST and 5:00 p.m. CST Monday – Friday

312-461-3716 – Chicago

414-362-6022 – Brown Deer

Investigative & Security Services (I&SS)

1-800-268-9373

BMO Harris Bank

We're here to help.

For Internal Use Only—Do Not Share With Customers

U.S. P&C Fraud Management

Fraud Alert

Figure 1A shows an ATM *without* any skimming devices

Figure 1B shows the same ATM *with* a skimming camera in place

Figure 1C is a close up of the device

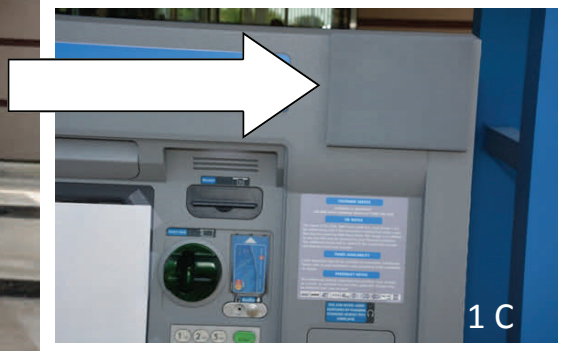

Figure 2A shows a different type of skimming camera in place

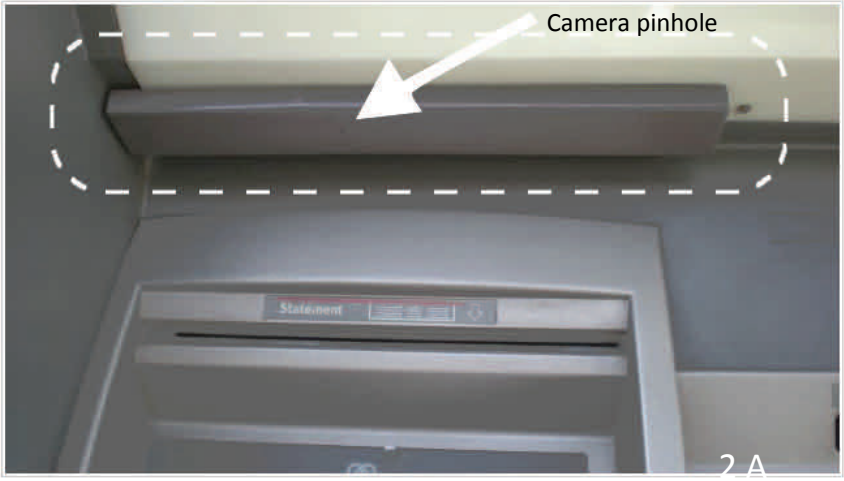

Figure 2B is what the camera looks like when removed