POLL PAD® SECURITY

theft of data from the Poll Pad. Further security is achieved through poll worker policies and procedures training that instruct poll workers to never connect any unauthorized devices to the Poll Pad or use the Poll Pad to install/run any unauthorized applications or access unauthorized websites.

Q: HOW DO POLL PADS HELP PREVENT VOTERS FROM CHECKING IN TO VOTE TWICE?

Each Poll Pad communicates with other nearby Poll Pads over an encrypted peer-to-peer network to sync check in data with all devices in a polling location. In jurisdictions that use live connections to ePulse on election day, this check in data is also sent to the server for transmission to Poll Pads in other polling locations. These data syncs ensure that as soon as a voter checks in on any Poll Pad, that voter is marked as "checked-in" on all other devices within the polling place to identify if a voter were to attempt to check in again.

Q: WHAT SORT OF SECURITY CERTIFICATION DOES THE POLL PAD UNDERGO TO BE APPROVED FOR ELECTIONS?

Each state has unique certification and/or approval activities for electronic poll books. KNOWiNK works with each state to comply with required certification/approval activities. Many states require assessment of the Poll Pad application and/or Apple's iOS by third party independent testing labs to confirm the safety and security of the Poll Pad solution. KNOWiNK has undergone numerous security reviews by Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS), and other federal agencies, as well as, private security firms.

Q: HOW DOES THE POLL PAD HELP PREVENT DECEASED PEOPLE AND PRISONERS FROM CHECKING IN TO VOTE?

To ensure the most current voter roll is in use, the Poll Pad is programmed and updated at regular intervals from the voter registration system. These ongoing updates ensure that any activities to revise the voter roll—including new voter registrations, purging deceased people, or purging those who have relocated—are included in the voter data loaded on each Poll Pad. The Poll Pad is programmed to guide poll workers to properly confirm each voter's identity in accordance with applicable laws and procedures so that only voters on the voter roll are allowed to check in to vote.

Q: A JURISDICTION DOES NOT ALLOW POLL PADS TO BE CONNECTED DURING VOTING BUT I SEE THE POLL PADS ARE CONNECTED TO EACH OTHER—WHY?

The Poll Pads communicate over an encrypted peer-to-peer network that shares check-in data with other Poll Pads within the polling location to prevent voters from checking in on more than one device during an election. For example, in a polling place that has deployed three Poll Pads to check-in voters, this peer-to-peer syncing ensures that once a voter checks in on one of the Poll Pads at the polling place, they cannot check in on either of the other two Poll Pads, helping to prevent a voter from checking in to vote multiple times.

Q: HOW DO THE POLL PADS HELP MAKE SURE A VOTER VOTES IN THE CORRECT PRECINCT?

The Poll Pad uses data provided by the voter registration system to confirm that a voter is allowed to vote in a specific precinct and/or polling place. If an eligible voter presents themselves to vote at the wrong precinct, the Poll Pad can be programmed to provide the address and directions to the correct precinct/polling place where the voter is registered to vote.

Q: IF SOMEONE VOTES ABSENTEE, CAN THEY ALSO VOTE IN PERSON?

The Poll Pad uses data provided from the voter registration database to ensure up-to-date voter status, including information on absentee or mail-in ballot status. If a voter has been previously issued a ballot or has returned an absentee ballot, the Poll Pad guides the poll worker to follow the state laws for the voter in that situation. In jurisdictions where a voter may vote a provisional ballot after having been issued an absentee ballot, the jurisdiction receives reports from the Poll Pad to allow them to compare to the voter registration database and ensure only one ballot for that voter is counted.

POLL PAD® SECURITY

Q: DO THE POLL PADS HAVE TO BE CONNECTED TO THE INTERNET? IS IT SECURE?

In some states and jurisdictions, Poll Pads connect to the Internet to send and receive data updates throughout election day. Poll Pads can report voter turnout data and check-in activity back to the board of elections in near real time. Poll Pads can also receive updated voter registration data from same day voter registration activities or returned absentee ballots.

Even if Internet connectivity is not used for election day, Poll Pads must be connected to the Internet before election day to receive updates for their operating system, updates to the Poll Pad software application, and to download the files required to view voter information. All data transmitted to and from the Poll Pad and its supporting servers is kept secure using the same type of encryption that safeguards network traffic for e-commerce, banking, and finance activities.

Q: HOW DO YOU PROTECT VOTER DATA?

Transmission of voter data between the Poll Pad and ePulse is encrypted. The Poll Pad application inherits the encryption capabilities natively provided by iOS and voter data within the ePulse application is saved into encrypted storage. Access to data within the ePulse application requires users to have a strong password, and application users are required to change their password at regular intervals. KNOWiNK routinely audits user access to the ePulse application and recommends that all its customers conduct regular user audits to purge users who do not need access to ePulse or the Poll Pad application.

Q: IS THERE A DIFFERENCE BETWEEN POLL PADS THAT USE CELLULAR MODEMS AND THOSE THAT ONLY USE WI-FI?

Cellular and Wi-Fi connections use different radio technology for the Poll Pad to send and receive data over the network: A cellular connection communicates directly over the Internet to send and receive data to and from the ePulse servers, while a Wi-Fi connection requires an interface with a router to send and receive data to and from the ePulse servers.

The direct cellular connection is generally more resilient because it does not require an additional router to connect to the Internet.

Note: Cellular Poll Pads also contain Wi-Fi radios which the Poll Pad uses to connect to a jurisdiction's infrastructure and avoid cellular data charges between election day events.

Q: IS THE DATA ON THE POLL PAD PROTECTED BOTH IN TRANSIT AND WHILE AT REST?

All data transmitted to and from the Poll Pad and its supporting servers is kept secure using the same type of encryption that safeguards network traffic used for e-commerce, banking, and finance activities.

The Poll Pad application has been developed to run natively on Apple iPadOS to integrate and manage the secure boot chain, system security, and app security capabilities of iPadOS and verify that only trusted code and apps are run on the device. Apple devices provide further protection for the Poll Pad application and data by storing all application data within an isolated, secure section of storage.

Q: IS IT POSSIBLE FOR SOMEONE TO STEAL VOTER DATA FROM THE POLL PAD USING SOME SORT OF WIRELESS DEVICE INSIDE OR OUTSIDE THE POLLING PLACE?

Encryption technology, configuration settings, policies, and procedures all work to prevent unauthorized wireless access to the data and software contained on each Poll Pad device. Data communicated between each Poll Pad and the ePulse servers is encrypted—such encryption ensures that no data transmitted wirelessly can be intercepted and decoded while in transit. Device-specific configuration and user policies and procedures prevent installation or use of additional software applications, and unauthorized connection of external devices, such as Bluetooth accessories, to the Poll Pad. Blocking the ability for such external devices to connect helps prevent

Continued on the next page...