



BY WILSON CHAO

Wilson Chao is President and CEO of WaveSoft. He can be reached at [wilson@wavesoft.com](mailto:wilson@wavesoft.com).

## DESIGN THE KILLER APP

Mobile POS applications can mean profits and pitfalls

**MOBILE POS APPLICATIONS** are becoming mainstream, as channel partners look for new ways to differentiate themselves in today's competitive landscape and the use of wireless networks in business settings increases. However, developing and deploying mobile POS applications is not as simple as porting over a desktop version of the POS software.

So how exactly should ISVs and VARs make a splash in the mobile POS market? While mobile applications can help companies differentiate themselves from more traditional competition, it can be a daunting task to combine the functionality of a traditional workstation into a user-friendly interface that delivers optimal usability and stability.

First, there is the programming component to consider: developers of mobile wireless LAN apps must take a traditional desktop POS solution and reprogram it to fit on a mobile device that typically has a 3.5-in. to 4.3-in. screen.

Therefore, functionality is critical, as users must be able to use the mobile application tableside in front of customers with the same ease of use as entering an order into a traditional POS system.

How does service typically flow in a restaurant? How many "clicks" should it take to place an order? These workflow concepts will help shape the interface and determine how it should be structured. It's important to consider the technological intricacies behind the applications. Mobile POS software runs on different platforms and must be designed to accommodate varying levels of screen resolutions.

Developers also need to consider the feasibility of running the new app on different OS platforms such as WinCE, iOS, and Android. In addition, mobile POS applications should provide open XML interface allowing for easy integration into any third-party server applications.

The security and reliability of a mobile appli-

cation is critical. Mobile POS solutions must offer end-to-end payment processing security to conform to the latest PCI compliance mandates. Data security is one of the most important aspects of a wireless application, as credit card numbers or other personal information could be transmitted over an unsecured network, making the business a target for theft or security breaches.

As if designing the application and determining the appropriate feature set is not enough of a challenge, developers also need to be ready to navigate the constantly changing wireless land-

scape of requirements, platforms, and protocols. This can be a difficult process, because almost as soon as a new technology emerges, a better, faster one becomes available which will eventually lead to higher development costs. That is why thin-client technology, such as terminal services, is often used as a tool to cut costs for mobile software development. Once completed, a mobile application

should be consistently updated to provide additional features and ensure compatibility with the latest wireless network and mobile platforms.

Known for providing a variety of benefits including—reduced wait times, increased sales, improved order taking accuracy, and greater table turnover—mobile POS solutions can provide a tangible return on investment. However, if the wireless network or mobile device isn't up to par, inevitably there will be some headaches. The wireless network being implemented must be reliable to ensure that users are able to connect wirelessly without any downtime or interruptions. Regardless of the type of mobile device used, reliability is key because the mobile solution is used at the point-of-action for both ordering and processing payments. Even the best mobile POS application won't help if a restaurant is using a mobile computer that has a short battery life, making it ineffective to complete an entire shift. **VSR**

**Mobile POS solutions must offer end-to-end payment processing security to conform to the latest PCI compliance mandates.**