

Going Mobile: The Growth of Device-Based Ecommerce in the 2018 Holiday Season

As shopping via mobile devices captures a greater share of e-commerce, experts are making bold predictions about the role cell phones will play in this year's holiday shopping landscape. Last year, over *one third* of online holiday shopping revenue came from orders placed on cell phones or tablets, totaling \$25.9 billion for the entire season (and \$7 billion for Thanksgiving weekend alone). Many industry sources predict that this year's mobile orders will continue to grow rapidly – capturing up to half of the e-commerce market share and comprising as many as two-thirds of online retail visits.

Some retailers are also integrating mobile devices into their brick-and-mortar shopping experience, particularly to alleviate long holiday shopping lines. Sam's Club has introduced a mobile checkout option called "Scan & Go" where customers can scan items as they add them to their cart and, when they're done, skip the checkout line and pay through the app. Target recently rolled out a similar initiative called "Skip-The-Line" – beginning in November, Target employees will be able to use mobile devices to allow customers to check out anywhere in the store. Walmart has announced it will offer the same services this holiday season. Its mobile cashiers will be armed with miniature Bluetooth printers so that employees can provide printed receipts for mobile checkout customers.

Retailers wishing to drive traffic to their mobile websites are faced with a number of data privacy and security considerations. Many retailers, for instance, use mobile apps to influence purchase decisions and collect data about consumer interest and habits, even if that consumer ultimately does not purchase anything in their mobile visit. Retailers should ensure that their apps follow best practices with respect to collecting and storing this information, including allowing customers to opt-out of tracking cookies and properly de-identifying any sensitive data collected (e.g. IP addresses).

Mobile orders, like all e-commerce purchases, are also susceptible to malicious hacking to obtain credit card information and other customer data. These breaches range from large-scale back-end hacking to smaller, one-off occurrences due to customers using public Wi-Fi (which is typically less secure than a private network). While factors like customers' choice of internet connection may be out of retailers' con-

trol, there are several ways retailers can make online shopping more secure – including using a secure online shopping platform and secure authentication for checkout; not storing any more customer data than necessary for returns or chargebacks; requiring e-mail account verification and strong passwords; employing algorithms to identify suspicious activity; providing order tracking; and training employees in proper cybersecurity measures.

As retailers take advantage of increased mobile traffic this holiday season, it will be important to revisit any relevant privacy or data security policies to ensure that reasonable measures are in place to avoid potential security incidents and to ensure that customer data is protected.