JAVELIN

The iPhone X is the Latest Reason FIs Need Customer-Informed Device Management

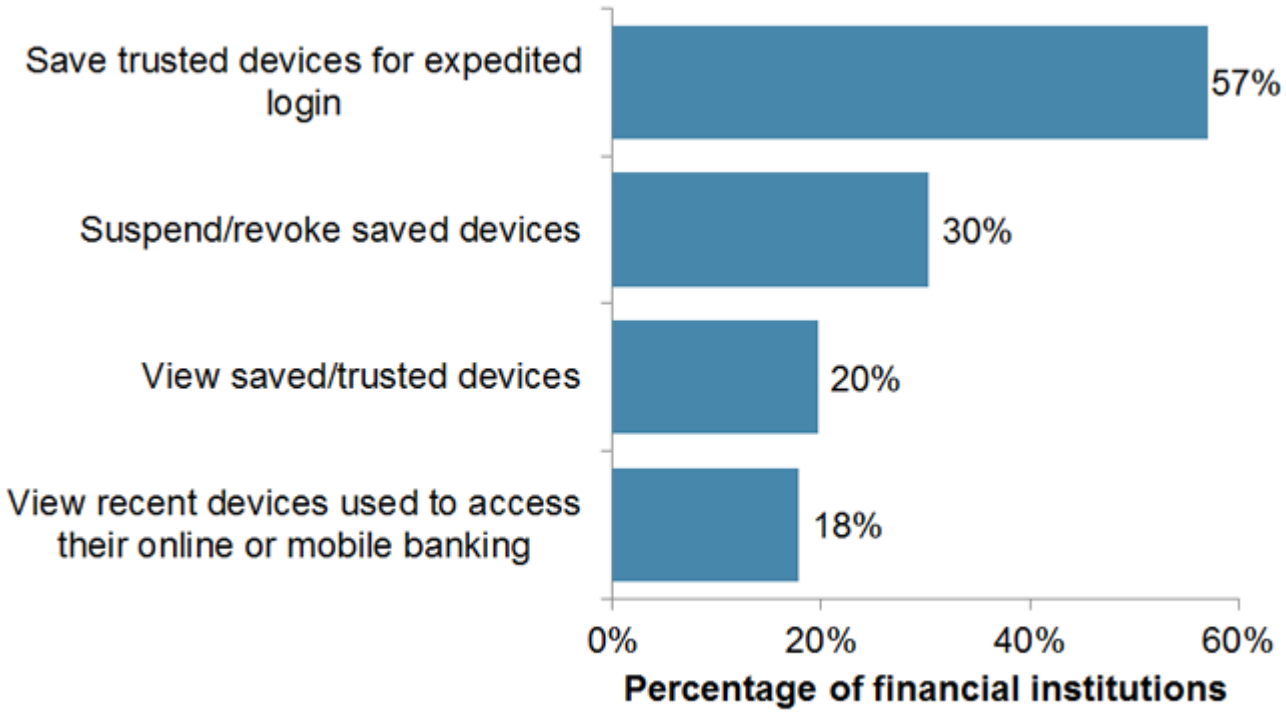
26 September 2017 By: Al Pascual

For those of you that did not get the opportunity to watch the recent unveiling of Apple's new product line you missed the same sorts of "oohs" and "aahs" we have come to expect. None were more emphatic, though, than those that followed the unveiling of the penultimate iPhone. The smartphone has become the center of our daily lives and the technology (and aesthetics) of these devices continues to evolve to suit our tastes and expectations. Our interest in the latest and greatest keeps us from settling for too long on the device that we seemingly can't put down today, and it drives us to desire the next shiny and feature-laden iPhone X (or Galaxy S8 for you Android fans).

Now that is all well and good, except that when you add our inability to stay loyal to our phones with the fact that we tend to bank across multiple devices that we sometimes lose, a level of complexity is created that impedes effective fraud prevention. If FIs want to be truly effective in leveraging the device as a means of distinguishing good transactions from bad, it behooves them to engage with customers who can say whether or not they've bought that new iPhone X and gave their antiquated, registered and bound iPhone 7 to a family member or friend (or simply traded it in), or even if the device was stolen – though why someone would want to steal something so old and useless is a mystery.

Companies that consumers are interacting with on a regular basis are taking on variations of this approach – Google is a great example of an organization whose actions we dissect in our latest report. Compared to Google and others, FIs are falling behind as evidenced by the fact that even for those institutions using device recognition, few have taken the next step in enabling accountholders to be active participants in the device management process. While over half (57%) of financial institutions in our most recent scorecard allow users to save devices for expedited login, just 1 in 5 (20%) enables accountholders to review devices associated with the account.

Only 1 in 5 FIs Offers Robust Device Management



Source: Javelin Strategy & Research, 2017

The device management portal is a valuable tool for preventing account takeover – which is up considerably from last

year. Without a complete view of recent devices used to access the account, suspending or revoking device access is typically done only for the device currently being used for access. While this is useful for users who intend to use a device for only a single access, it does not help accountholders whose device has been lost or stolen. Moreover, being able to review recent devices can alert users to unauthorized accesses that may have slipped through authentication safeguards. This works best when paired with alerts of new devices and suspicious logins – tools again that depend on engagement with the customer.

Consumers aren't going to slow the rate at which they switch devices. If anything, they will be adding more devices to their account – think virtual assistants and other connected devices – which will only make matters worse. So yes, there are new features in these devices that we need to contend with that tend to distract practitioners as well as everyday consumers (the impact of Face ID on the authentication landscape is a great topic for another day), but the implications of this simple underlying dynamic have yet to be addressed by most institutions. Our collective technolust is a distracting, almost ridiculous phenomenon, but what it means for protecting accounts is clear.

All we need to do is ask and listen.

---

javelinstrategy.com inquiry@javelinstrategy.com 925.225.9100