ZoOm® Interface: Logo & Version

Maintaining Consistency & Increasing Security

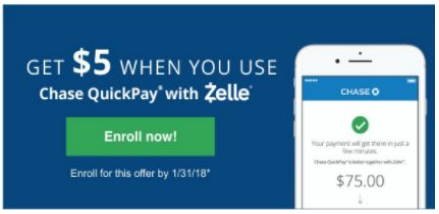
ZoOm has been honed over many years with user feedback from 158 countries and on over 1700 unique smart device models. The result is a fast, intuitive and trusted interface that is recognized by users and relied upon by major banks, enterprises and governments around the world.

Just like co-branded Bank + VISA, MC or AMEX Cards, the very small but consistent presence of the ZoOm logo creates trust and ensures a consistent user experience. Users are concerned about privacy and want to know they are interacting with a genuine ZoOm interface, and that their biometric data will be respected, encrypted and handled properly (think GDPR).

The ZoOm logo is a registered trademark, so if a bad actor were to make a fake ZoOm interface and attempt to phish users, FaceTec would instantly have the app stores remove the offending app for trademark infringement.

“But Big Bank XYZ will never accept a 3rd-party logo in their interface.”

Yes they will, but only when that 3rd-party logo represents a great user experience, trusted security and increases customer loyalty. The reality is, if a bank wants the best security and intuitive user interface, they must use ZoOm; no other universal biometric software platform even comes close.



Banks co-brand with many strategic partners. ZoOm is the next trusted brand on the list.

FICO SCORE
experian
TransUnion
NCR
gemalto

RSA SecurID®
PayPal
Zelle®
venmo
ZOOM

Interface Increases Security

Banks already co-brand with security companies, namely RSA and Verisign. There is significant precedent for the ZoOm logo to be included as a trusted security partner**.**

An argument is often made that hiding or obfuscating the version number of a piece of security software is desired. The reasoning is that hackers won't know exactly what they are up against. This is a completely false argument. In apps that are widely distributed (i.e. App Store/Google Play), there is nothing stopping determined hackers from rooting any iOS or Android device and inspecting iOS and Android app packages at the binary level. There is absolutely no security advantage by hiding the ZoOm version number.

On the contrary, displaying the ZoOm logo and SDK version number inside the ZoOm interface improves security. The ZoOm logo and SDK version number comprise a consistently located watermark, and can be seen over the user's ZoOmed face in any video, photo or screenshot taken from an authentication session. ZoOm algorithms are trained to detect this watermark. When this is presented to the camera, this is yet another way we detect spoof attacks from screenshots or (rooted/non-rooted) screen records. Detecting attacks like these can be used to alert a bank and their correct user.

Finally, if someone was ever able to spoof ZoOm in a recreatable way and post a video online showing the spoof method, FaceTec would be able to see the version number and know if that specific vulnerability had been addressed in future versions. This protects the ZoOm brand and the brands of all of ZoOm's customers.