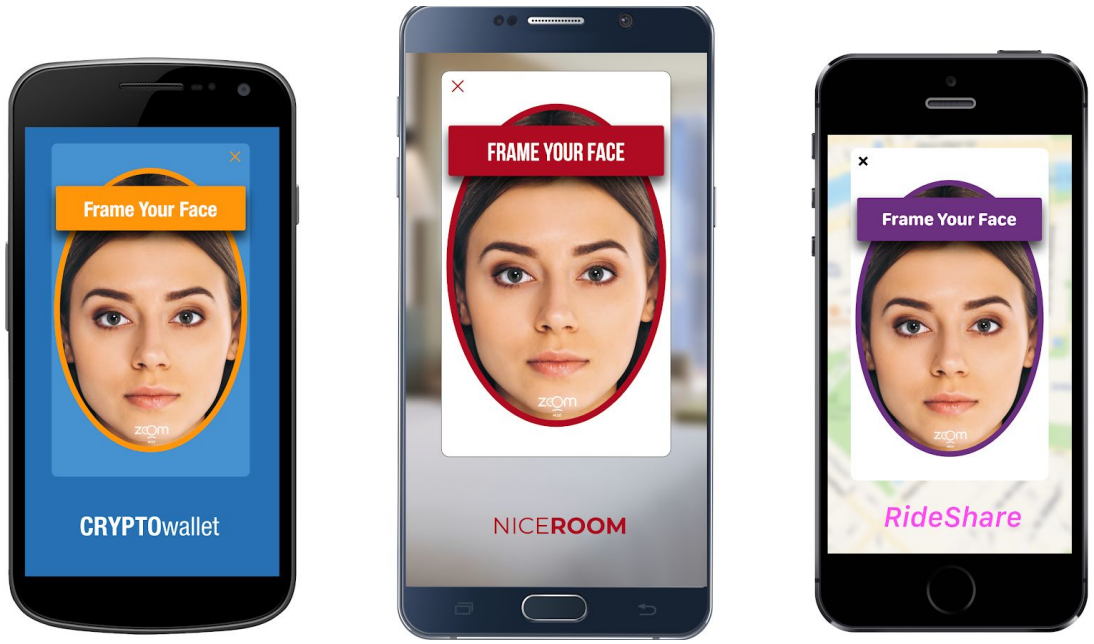
ZoOm® Interface: Logo & Version

Maintaining Consistency & Increasing Security

ZoOm has been constantly improved over many years from user feedback in 170 countries, and on over 2000 unique smart device models. The result is a fast, intuitive and trusted interface that is recognized by users and relied upon by major organizations in banking, transportation, ID/access management and governments around the world.

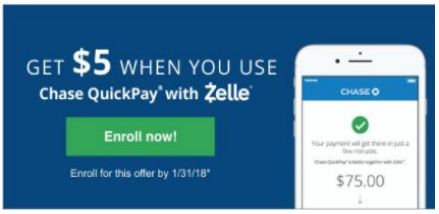


Just like co-branding from VISA, MC or AMEX on major bank cards, the very small but consistent presence of the ZoOm logo creates trust and ensures a consistent - and safe - user experience. Users are concerned about privacy and want to know they are interacting with a genuine ZoOm interface, and that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

The ZoOm logo is a registered trademark, so if a bad actor makes a fake ZoOm interface and attempts to phish users, FaceTec can instantly remove the offending app from App stores for TM 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. In biometric security, ZoOm is the trusted brand.

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 security software version number is desirable because hackers won't know exactly what they are up against. This argument is completely false. In widely distributed apps (i.e., App Store, Google Play), there is nothing stopping determined hackers from rooting iOS or Android devices and inspecting app packages at the binary level. There is absolutely no security advantage in hiding the ZoOm version number.

But displaying the ZoOm logo and SDK version number inside the ZoOm interface actually *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 presented to the camera, this is yet another way we detect spoof attacks from screenshots or (rooted/non-rooted) screen records. Critically, detecting attacks like these can be used to alert a bank and their correct user.

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

Summary

For marketing, it might seem counterintuitive to co-brand a highly-recognized product with a lesser-known expert brand. But co-branding is as old as advertising itself and can create even more confidence in the primary brand. By highlighting each brand's strengths, the primary product is viewed as improved and provides more recognizable value. ZoOm has built well-deserved credibility within the security industry as the most secure face biometric available. It is the only face biometric to achieve Level 1 & 2 Liveness Certification in the ISO-guided Presentation Attack Detection tests by the world's only NIST/NVLAP-certified testing lab, iBeta. For any organization seeking validation that their products are secure, there is no better security partner than FaceTec, and no better biometric than ZoOm.