



Boloro is working to make you Safe and Secure

Everyone is doing everything remotely online, and everyone is concerned about social distancing. The Internet was never designed for secure transactions and other risky activity, and Operating Systems are regularly subjected to malware. SIM Swaps, email hacks, malware, man-in-the-middle attacks and other forms of fraud are rising dramatically, costing many tens of billions of dollars globally per year. In addition, it can be dangerous to touch a public Point of Sale device, ATM keypad, finger scanner or anything that could spread the coronavirus.

Boloro Authentication leverages the secure signaling channel of the mobile network operator, push USSD or network initiated USSD, to separate the authentication from the activity itself. Boloro also works with RCS or any channel that is sufficiently secure and available. With Boloro, all activities can be conducted safely and securely on the personal mobile handset, eliminating sole reliance on the Internet and eliminating physical contact with a public device or screen. Boloro is compatible with all mobile phones, including smartphones and feature phones, and easily deployed via APIs for local hosting and / or cloud-based hosting.

Mobile Network Operators and aggregators should adopt Boloro Authentication and monetize an existing channel for new revenue from new and existing customers across numerous use cases, including: online banking, digital payments and eCommerce, as well as the avoidance of touching public Point of Sale machines, ATM keypads, finger scanners and other public devices by putting all activities safely and securely on the personal mobile handset.

Boloro is ready to work with you to make our world safe and secure!

Boloro Global Limited

425 Park Avenue, 39th Floor, New York, NY 10167, USA
E: contactus@boloro.com **W:** www.boloro.com