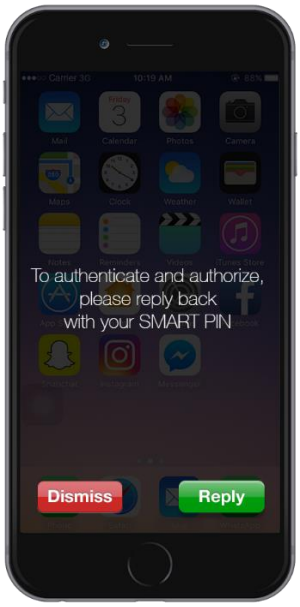
Superior Security of Boloro's Multi-Channel and Multi-Factor Authentication is Ideal for Protecting Bank Apps and Avoiding Card-Not-Present Fraud

Boloro's major differentiation in ensuring ID and transaction security is in its multi-channel approach, segregating the transaction and authentication medium/channel and the device, avoiding the "**single point-of-failure**". Other security solutions are exclusively based on encryption over the Internet channel, where individual and organized fraudsters are routinely preying on and ambushing vulnerable users transacting on the same inherently flawed road (the Internet) by exploiting the slightest weaknesses. Boloro's Patented Authentication Process completely avoids the Internet – the "road" used by remote fraudsters - and Boloro cleverly leverages the isolated and secured signaling channel used exclusively by telecoms for their internal purposes.

When a transaction takes place on the Internet or data channel, the Boloro platform pushes an **Authorization Session** over the telecom signaling channel as a **Flash Message** in **Real-Time** to the specific handset and mobile subscription of the user without touching the operating system (OS). Once the user enters its **Memorized PIN** to validate the transaction, the session ends leaving no trace of the message on the user's handset. Boloro always validates the origination of the PIN and the PIN itself before an authentication is successfully processed, with these key differentiators:

- The communication can't be intercepted by any cyber fraudster due to private point-to-point secured network between financial institution and telecoms, and instant session based real-time response from the actual user handset;
- A5/3 block cipher has been standardized for over the air communication and no practical attacks are known against A5/3;
- Last mile frequency of mobile user becomes a moving target and prevents any mass eavesdrop attempts from far away location;
- Boloro's Authentication Flash Message never interacts with the handset's OS and is therefore immune from any OS malware;
- Boloro ensures multiple factors of "what you have (physical mobile phone)" is validated and also securely collects "what you know (virtual element, the Memorized PIN)" using a secure, separate channel "bypassing the Internet"; and
- Boloro does not require any personal data from the user, avoiding the catastrophic consequences of biometric data breaches.



Boloro is Secure, User-Friendly and Instantaneous Authentication

The security of the signaling layer, combined with Boloro's patented authentication technology, creates an impregnable lock that protects online banking and payment apps, as well as logins for data, emails, social media and other activity. Boloro provides ultimate protection without requiring any personal data from the user, putting ATM-like security in the palm of your hands.

Boloro Global Limited
@ Rise NYC, 43W, 23rd Street, 2nd Floor, NY, NY 10010, USA
ContactUs@boloro.com www.boloro.com