Q2 Gro: Frictionless Account Opening Made Secure

The need for cybersecurity is nothing new, but as banking traffic—including account opening and onboarding—continues to move into the digital space, it's crucial that financial institutions have the proper security controls in place. A proven leader in fraud prevention, Q2's approach to account opening includes a multifaceted approach to security while maintaining positive user experiences.

In-Application Security

Our account opening solution, Q2 Gro, has a robust set of security capabilities built into it. Gro's workflow is optimized to let the good in while keeping the bad out, including SMS verification, KYC, email collection/validation, and customized application kick-out rules.

Gro also integrates with best-in-class providers in the identity space to provide maximum flexibility. We currently integrate with more than 15 KYC and funding verification providers, including the recent addition of Socure and Alloy integrations.

Enabling utilization of:

- Machine-learning algorithms comparing against multiple data sources
- Step-up authentication
- Custom decisioning steps
- Regional checks, to determine users are in a serviceable area
- Qualifile risk management assessments

Our existing customer authentication process moves existing customers to pre-authenticated channels. This helps reduce friction, providing a superior user experience while still focusing on fraud prevention.

Complete Access to Data and Analytics

Q2 Gro makes all account opening data and metadata available to customers—including IP addresses, GPS coordinates, and repeat-attempt tracking. All data is integrated easily into third party tools to give additional flexibility and reporting capabilities.

Funding Controls

Q2 Gro reduces fraud exposure by controlling funding limits at both the product level and the payment method level. Our integration with Plaid verifies the ownership and sufficiency of funds.

Infrastructure-Level Protection

At the infrastructural level, we have DDOS protection through AWS. We also have geographic controls in place, determining geographies where whitelisting is available.

Administration Controls

Q2 Gro features robust entitlements and roles, with your FI controlling who has access to what information, with full admin audit logs and detailed audit reports available.

Synthetic Fraud Prevention

The key to uncovering the false identities used in synthetic fraud is to leverage and compare multiple layers of data from a variety of sources. Our data-rich approach to account opening recognizes fraudulent identities before they're able to open an account.

Our existing customer authentication process moves existing customers to pre-authenticated channels. This helps reduce friction, providing a superior user experience while still focusing on fraud prevention.

For more information, go to Q2.com or call (833) 444-3469.