SECURITY

Prevent Banking Fraud with Multi-Layer Security from Q2

Fraud attempts and other security threats against financial institutions (FIs) are increasing, and criminal techniques are becoming more sophisticated. Q2's multi-layer security products bring real-time fraud protection to banks and credit unions, along with a seasoned team of professionals dedicated to best practices. Q2 machine learning and behavioral analytics help drive the responsiveness of many of our security products and systems tests. Our range of security options will bring your institution even more effective operations.

Key Features and Benefits

- Proactive security using machine learning and behavioral analytics prevents funds from leaving an institution
- Systems testing to determine exploitation points within your institution—and to thwart social engineering threats
- Automated fraud alerts to notify staff immediately
- Seamless, integrated security for more efficient and effective back-office operations

Innovative Security for Better Digital Banking

Q2 has superb security options for banks and credit unions, including highly effective products designed to protect both FI and account holder assets. **Q2 Sentinel** uses behavioral modeling to track anomalous activity and will suspend suspicious transactions before they can leave your institution. Powerful prevention based on behavioral analytics isn't just limited to Q2 Sentinel, **Q2 Patrol** leverages user behavior around login activity and device details to identify potentially suspect sessions and requires further authentication around high-risk activities. Our **Social Engineering Assessment** determines exploitation points within your institution, helping your staff learn to avoid falling prey to outside threats. And then there's **Q2 Services and Support**—our team of experts can help you optimize existing security and operational procedures.

Product Details

Q2 Sentinel monitors and analyzes transactional and user data in real time to identify and suspend suspicious transactions **before they take place**. Transactions could include ACH payments, external transfers, and wires. Sentinel determines whether login events and transactions are suspect based upon a wide range of characteristics which are analyzed against historical online account holder information.

Q2 Sentinel also utilizes policy-based decisions for certain transactions to determine whether an account holder's past transaction approval history supports approval of current transactions. This means Q2 Sentinel can intercede and prevent a possible fraudulent transaction from going through. From 2015–2016, for example, 93 percent of funds scored as "suspect" by Q2 Sentinel were retained. This proactive capability is unique.

An ideal security solution for the mobile-first world, Q2 Sentinel monitors anomalous behavior with logins and transactions generated on the mobile channel just as it does other channels, and the same behavioral models are used to determine whether a transaction generated on the mobile device is suspect or not.

Q2 Patrol monitors account holder behavior, can quickly identify suspicious activity, and protect non-transactional, high-risk events. When Q2 Patrol identifies potentially fraudulent sessions, it allows your institution to require further authentication—such as a secure access code or token—to execute certain high-risk events. Doing so, Q2 Patrol ensures only the authorized account holder can proceed.

Q2 Patrol will give further insight by providing reporting based on individual user and session details, helping to meet Know Your Customer requirements. Information found in the reports will include geolocation, session timestamp, and IP address. Patrol also adds extra value by providing account holders with access to details around their previous sessions and possible fraud attempts without involving your staff.

83%

increase in fraudulent transactions and behavior in 2016*

*Q2 Fraud Report, 2016.

The Q2 Social Engineering Assessment tests your organization for breaches through people-focused attacks, like phishing. Our assessment is an ideal way to educate staff on what to look out for and to avoid when it comes to cybercriminals trying to infiltrate your institution. We create and administer authentic, multichannel simulations of the latest most effective social engineering attacks to help identify and significantly lessen risk within your institution. Simulations meet regulatory and compliance requirements for validating security controls, and a detailed report identifies and describes threats, gaps in employee knowledge about scams, and provides actionable recommendations.

Q2 Services and Support can help our Q2 Online Banking platform customers optimize existing security and operational procedures, bringing alignment with best practices and putting our extensive experience to work for you. Q2 even has a fraud response team dedicated to staying on top of fraud trends to ensure optimal performance for our customers.

Security and the Q2 Digital Banking Platform

While third-party solutions are only able to alert you when an issue arises, Q2's suite of security products are integrated into our Online Banking platform and can seamlessly integrate with back-office procedures for highly effective, real-time, multi-layer cybercrime prevention.

Security for Any Device

Whether your account holders are conducting transactions on a desktop, tablet, or smartphone, their banking activity will be secure with Q2.

We can help.

For more information on Q2's security solutions, go to **Q2ebanking.com/security** or call **(512) 275-0072 ext. 2**.