

# Security & Risk Management

Smart, scalable, around-the-clock protection

The fraud and risk landscape is complex and ever-changing. To protect your account holders, assets, and reputation, you need proactive, sophisticated security solutions. You need tools that learn and adapt, that stop emerging threats before losses occur, and that keep your data safe from cybercriminals.

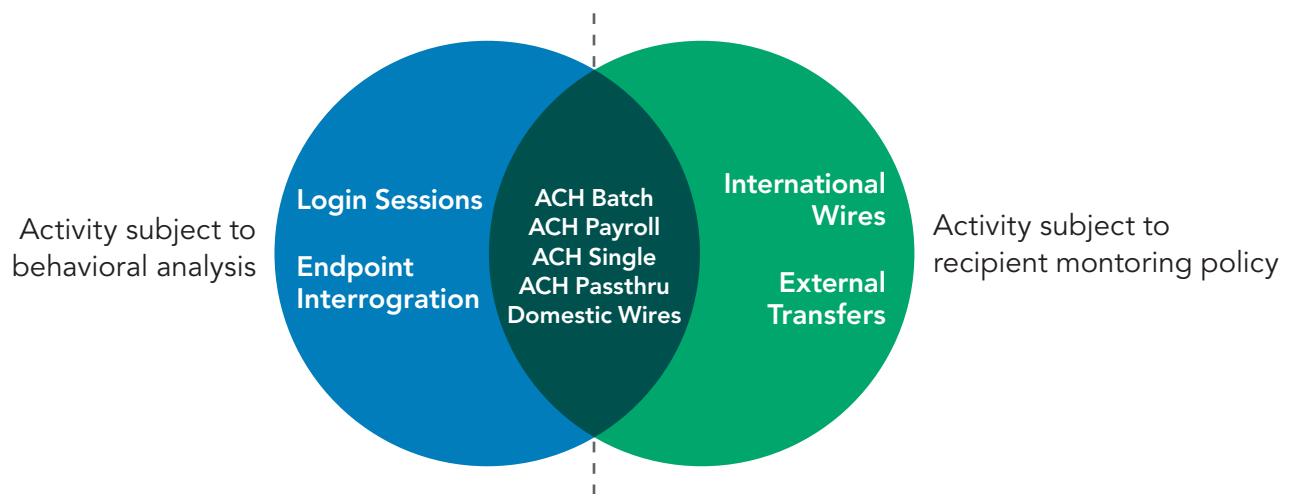
## A comprehensive approach to security

Minimize exposure and losses related to fraud with an intelligent, multi-layered, end-to-end suite of native, data-rich security solutions.

### Q2 Sentinel

#### Stop fraud by learning your account holders' behaviors

Q2 Sentinel is a behavioral analytics solution that measures and compares the details of requested transactions versus typical behaviors to provide real-time security for ACH transactions, wires, and external transfers at the user level. Suspicious transactions are flagged in real-time for review by your financial institution.



## Sentinel scores transactions based on behavioral analysis, policy, or both

#### Behavioral-based

**Login history** – Sentinel considers historical activity including day, time, state, and IP address.

**Transaction details** – Sentinel considers deviations from previous activity such as dollar amount (including minimum, maximum, and median values in ACH files), creation and authorization patterns, recipient location, Fed districts, and more.

**Endpoint interrogation** – Sentinel considers the user's device details, including browser, operating system, and the software installed on the device.



## Policy-based

**Recipient monitoring** – Sentinel analyzes policy-based rules, such as whether the transaction is to a single and/or new recipient, or if a large percentage of a transaction is going to a new recipient.

## Q2 Patrol

### Add an additional security layer with authentication requirements

Similar to Sentinel, Q2 Patrol continuously monitors user behavior, determines account holders' patterns, and quickly responds when it sees a deviation in behavior that could indicate an imposter. However, should a security concern arise, Patrol will require further authentication from account holders around certain high-risk, non-transactional activities.

## Q2 Trustview

### Avoid the pitfalls of manual data management and provide the cybersecurity your account holders expect

As the most advanced data protection technology on the market, Trustview safeguards critical user data with a multi-layered approach combining blockchain and machine learning capabilities. How it works:

**Blockchain protection** – Storing personal information on a private, low-latency blockchain network makes data-at-rest useless without authorization.

**Minimal human touchpoints** – People make mistakes, so it's risky for them to interact with complex data networks. Trustview uses machine learning and behavioral analytics to minimize human contact.

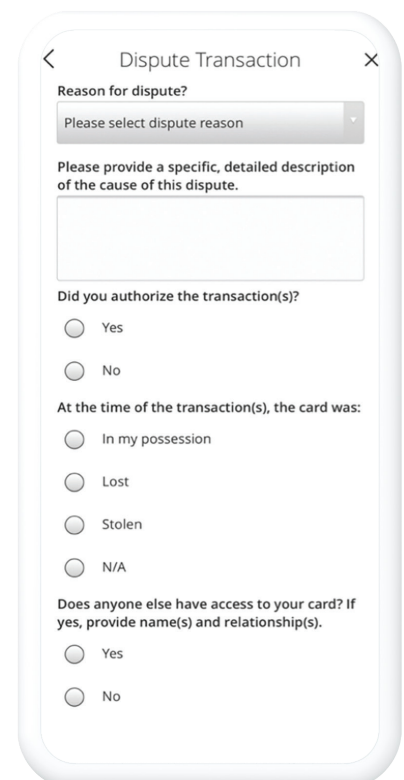
**Layers of security** – By placing multiple steps between would-be attackers and your data, our platform offers protection within and beyond Q2's data centers.

## Integrated fraud and risk management

Q2 offers easy **dispute initiation and tracking for digital banking users**, as well as integrated tools for streamlining risk reviews, and a comprehensive positive pay solution.

Account holders want easy, seamless, and secure financial experiences, and they want them from you.

You can meet their needs **securely** and **simply** with a single, smart digital banking platform. Q2's focus on creating positive, relevant experiences helps you become a reliable partner on their life-long financial journeys.



The screenshot shows a mobile application interface for disputing a transaction. The title bar at the top reads "Dispute Transaction" with a back arrow on the left and a close "X" icon on the right. Below the title bar, there is a section titled "Reason for dispute?" with a dropdown menu that currently displays "Please select dispute reason". Underneath this is a text input field with the prompt "Please provide a specific, detailed description of the cause of this dispute." Below the text field, there are three radio button options: "Did you authorize the transaction(s)?" with "Yes" and "No" options. The next section is "At the time of the transaction(s), the card was:" with radio button options for "In my possession", "Lost", "Stolen", and "N/A". The final section is "Does anyone else have access to your card? If yes, provide name(s) and relationship(s)." with radio button options for "Yes" and "No".

For more information, go to [Q2.com](https://www.q2.com) or call (833) 444-3469.