Webinar

Using Security to Lock in Commercial Banking Customers

June 2017

Commercial banking is a market opportunity that financial institutions (FIs) should not ignore. Tens of billions of dollars in FI revenue can be attributed to commercial banking services, with 70% of that coming from small to mid-sized businesses. However, being able to target, acquire, and retain commercial banking clients is difficult when security isn't properly addressed.

Q2 recognizes this potentially revenue-rich market and has developed tools to help turn these businesses into viable targets for smaller FIs. With multilayered security to address different exposure points and risks, Q2 leads the industry in delivering secure and accessible digital banking experiences.

Context

Q2's Eric Jewell and Mike Hayes discuss the role that security plays in attracting and supporting commercial banking accounts.

Key Takeaways

Q2 offers a user-focused approach to security that employs four different layers.

FIs need to deliver practical security that balances user convenience for a wide range of clients—all within an experience tailored to account holder needs.

Q2's multilayered security allows all customers, regardless of size, to personalize most features to meet their individual requirements.

Layer 1. Perimeter Security
Perimeter security relates to a series of actions that are set in motion before a user can access data, move money, or make transactions. With features including device identification, malware detection, user authentication, and anti-phishing recognition, this layer is designed to proactively detect fraud before it occurs.

> "What if you were able to transition from talking about security as something that we reluctantly have to endure and accept to, instead, being an organizational asset that adds value?"
>
> — Eric Jewell, Q2 Product Owner

Layer 2. Behavioral Security
The next layer, behavioral security, monitors and remembers user behavior to quickly take action when deviations from the norm are spotted. Q2 Sentinel was built to actively restrict transactions when they occur outside of expected user behavior. Deviations include irregular transaction locations, times, amounts, or types of purchases.

At this level of security, Q2 Patrol might prompt users to complete a secondary verification process, based on the occurrence of certain high-risk events. For example, an admin logging in from an unknown device or IP address in the middle of the night attempting to add a sub-user may get prompted for MFA, but another customer following historical behavioral patterns would not be prompted.

Layer 3. Transactional Security
The third layer, transactional security, looks at who in particular is conducting the transaction and transaction limits. It examines policy-level descriptions around those transactions, ensuring that they're consistent with defined policies. The factors include levels of approval and roles. These are closely monitored and alerts or additional authentication (through tokens, for example) are sent based on potential threats or the need for approval.

Layer 4. Entitlements Security
Entitlements security makes up the fourth and final layer. Focusing on business controls, business-level feature access, role-based assignments, segregation of duty, and much more, this layer is often the most complex piece of security and requires the most education.

Q2 uses entitlements security to differentiate itself.

Traditionally, digital banking platforms need an organization to establish a series of complex rules that direct a user's ability to successfully perform commercial transactions. The problem with this model is that, as the number of accounts and possible actions increase, users get lost in the process.

- Q2 investigated the different personas that use digital banking platforms and then developed an approach to entitlements security that's intuitive, easy-to-use, and practical.
- Q2 offers two different entitlements security options: simple and advanced. Typically, the simple model can support small to midsized businesses, while the advanced model is better suited for larger corporations.

Not all customers and end users are created equal.

Using four sample personas, Q2 is able to address the variations in complexity a user might need.

Persona 1. The Sole Proprietor
The digital banking needs of a sole proprietor will often mirror the requirements of an individual consumer. These might include quick access to balance and transaction information, the ability to transfer money between accounts on the go, bill pay, and limited ACH.

Additional security tools such as device identification, malware detection, Touch ID, and frequent alerts help them remain secure and aware of any unusual activities.

Persona 2. The Limited Liability Company (LLC)
Because LLCs come with an increase in employees and accounts, they often represent a fairly significant step forward in complexity.

The LLC requires the same digital banking needs as the sole proprietor multiplied tenfold. They need more sophisticated ACH and wire capability, payment methods, as well as the ability to perform multiple transfers at once across multiple accounts.

Their security profile intensifies as well, requiring positive pay, more token use, the management of secondary users at the customer level, and the ability to manage account and transaction access.

Persona 3. The Corporation
Corporations and the controllers who run them need access to a wide array of services—including advanced security, entitlements, reporting, transfers, payments, and more.

Corporations require the ability to segregate duties and roles, hold a large number of accounts with many users, to mandate high-volume money movements, and to perform other advanced functions to keep their digital banking moving swiftly.

On the security side, they need sophisticated tokens, granular entitlements, approval controls, source origin control, and role-based user management.

Persona 4. The Financial Institution
Financial institutions need the tools and features to support all of the above-mentioned personas. FIs require flexible and configurable digital banking functionality—and security solutions to fit every kind of client's needs.

Additionally, FIs need tools like Q2 Sentinel and Q2 Patrol to monitor behavioral analytics and identify high-risk events. They also require intrusion detection, sophisticated reporting, and anomalous transaction detection.

Q2's digital security measures are similar to securing a physical property.

Offline security provides a useful analogy. Consider the following four physical counterparts to our perimeter, behavioral, transactional, and entitlement security:

First, a strong sentry around the perimeter of the property and a high wall around the foundation are created to keep the bad guys out in the first place. Within the property there are laws and rules that keep order and safety. And finally, a net contains intruders in the event that they get inside.

Keep in mind that behavioral security will be found throughout the layers, gathering information so that it can, as needed, recognize intruders and cast the net to stop them.

Did you know?

There are nearly 35 security alerts native to the Q2 Platform, covering everything from new payment recipients and forgotten passwords to fraudulent activity.

Q2 Sentinel continuously monitors, learns, and then models user behavior to detect irregular actions. Over time, it provides deeper insights and more accurate models of account holder behavior.

Q2 Patrol is also a behavior-based security solution; it leverages login activities and device details to score banking sessions. Q2 Patrol adds another level of security by automatically requiring further authentication via a secure access code or token when users attempt to initiate certain high-risk events.

> "We've invested significant time and resources to make sure that we understand the personas that use our platform. We're looking at data from over 1.5M businesses that use our software each and every day. We engage directly with our clients and their end users to understand not just how they use our software—but how they think about completing the tasks."

— Eric Jewell, Q2 Product Owner

Biographies

Eric Jewell
Product Owner, Q2

With over 11 years of digital banking experience and five years in commercial lending with BB&T, Eric joined the Q2 team in 2015. Eric has since provided the vision for Q2 person-to-person (P2P) payments and security solutions. He ensures that financial institutions and their account holders enjoy a digital experience that is as safe as it is convenient. Eric holds both MBA and undergraduate degrees from the University of South Carolina.

Mike Hayes
Strategic Account Advisor, Q2

Mike joined Q2 in 2014 after spending a combined 13 years in digital banking and financial services. Mike's expertise lies primarily around corporate banking and cash management. He currently focuses on providing strategic guidance to larger financial institutions around complex, resource-intensive processes and needs. Mike came to Q2 with an undergraduate degree from Loyola University and a graduate degree from John Jay College in New York City.

Robby McWilliams
Director, Product Management, Q2

In March 2016, Robby joined Q2, bringing over 20 years of experience in banking and financial services. Robby draws on his experience in community banking, at what was First American Bank Texas, to lead the Business and Corporate Banking product management team. Their sole focus is on providing solutions that equip community and regional banks with the tools necessary to compete to win in the commercial banking landscape.

For more information, go to q2ebanking.com or call (512) 275-0072 ext. 2.

