CUSTOMER SUCCESS

Q2ebanking

Building One of the 500 Fastest Growing Businesses in America with Authentication from Symantec

How can community banks and credit unions compete with megabanks in offering secure mobile and online banking? They can license a ready-to-customize platform called Q2ebanking. It includes a validation and ID protection service from Symantec. Success in the marketplace has made Q2ebanking among the 500 fastest growing companies in America for the past two years.

How David beats Goliath

Megabanks—with hundreds of billions and sometimes trillions of dollars in assets—are tough to beat. They establish branches all over and set the standard for convenience.

But when the banking industry developed ATM networks, the convenience of having easy access to cash became commoditized.

Then online and mobile banking came into being. Now it's possible to access a bank account anytime, anywhere. In addition, many merchants will give customers extra cash from their account when a debit card is used for purchase—so growing numbers of customers rarely have the need to visit a physical bank. They can manage their accounts from a computer screen or smartphone, and get cash on the run.

With so much at stake, big banks can invest millions of dollars in developing easy-to-use interfaces and convenient online services. What chance do smaller to mid-size community focused banks and credit unions have?

Enter Q2ebanking. "What we provide is a highly secure single software platform that enables community-focused banks and credit unions to offer online, voice, and mobile banking to customers," says Mickey Goldwasser, vice president, marketing at Q2ebanking. The banks and credit unions utilize Q2's platform for ebanking and then customize its interface with their own logo, look, and feel.

The other side of convenience

But as bank and credit union accounts get easier to access anytime, anywhere, cybercriminals are developing more effective ways to access these accounts fraudulently. The media, public, and government have taken note, because if user confidence is affected, the growth of online and mobile banking could be threatened.

ORGANIZATION PROFILE

Website: www.q2ebanking.com
Industry: Financial Services
Headquarters: Austin, Texas
Employees: 180

SYMANTEC SOLUTIONS

Web Security

Why Symantec?

· Industry-leading reputation

· Cloud-based service easy to deploy

· Flexibility of hard or soft authentication tokens

"If customers or members don't feel secure, they're not going to use the channel," notes Adam Anderson, Q2's chief technology officer. "They have to feel that it's a safe environment. That's why we want to provide financial institutions in our target market with security technology equal or superior to what big megabanks can offer—we feel that security can be the differentiator."

Says Ward Howell, director, security solutions consulting at Q2: "We have a different vision of security tools—they need to be aimed just at community banks and credit unions. It's not one size fits all, it's one size fits exactly right. We've created products, solutions, and processes to make sure that banks and credit unions have really good security tools."

The ultimate issue is trust, Anderson points out. "People want to trust the institution they bank with. When they walk into a branch and see the vault, they feel that everything is safe. They need that same type of feeling when they go through the e-channel."

Security that's overlapped and layered

It's not enough to protect customers by requiring a name and password, says Anderson, even when the software can detect a sign-on occurring from a different computer, and challenges the user with an additional security question.

"We've given up on using just the set of authenticating technologies at the point at which transactions are made," Anderson says. "The market has failed to address the fact that any of those technologies can be overcome given the amount of research, time, and effort that an attacker wants to spend."

Those authenticating technologies aren't obsolete and are still useful, Anderson adds. "It just means that if you want to have an overlapped and layered approach to security, you need those fundamental identification technologies on the authentication side, and you need to make an investment in authorization and evaluation technology on the transaction side."

SOLUTIONS AT A GLANCE

Key Challenges

- Earn and keep the trust of online and mobile banking customers
- Provide easy to use yet effective and secure authentication
- Create enhanced security as a differentiated benefit

Symantec Products

- Symantec™ Validation and ID Protection Service (VIP)

Symantec Services

- Symantec Essential Support Services

Technology Environment

- Applications: Web-based online banking application built on the latest technology

BUSINESS RESULTS AND TECHNICAL BENEFITS

- One of 500 fastest growth rates in America, enabled in part by secure authentication
- 912% growth supported in past three years
- Faster time to value by being cloud-based, with no infrastructure to deploy on-premise
- Flexibility to serve different use cases with hard or soft tokens for authentication

Stopping fraud before it starts

With that in mind, says Howell, "we recently launched a risk and fraud analytics product that does real-time decisioning on fraud detection and anomaly monitoring. It tracks the IP addresses users are logging in from, analyzes and monitors typical behavior for that user, and verifies identity through a multi-factor approach that includes Symantec Validation and ID Protection Service (VIP, formerly VeriSign™ Identity Protection Authentication Service)."

Q2ebanking had considered other services, but chose Symantec VIP "because we felt it was the best solution," Goldwasser explains.

"We want to provide banks in our target market with security technology equal or superior to what big megabanks can offer—we feel that security can be the differentiator."

Adam Anderson
Chief Technology Officer
Q2ebanking

If a transaction cannot be verified as legitimate, Howell observes, "our solution proactively suspends it in real time, so money doesn't leave a bank or credit union until it is verified."

Symantec™ VIP delivers cloud-based strong authentication for Q2ebanking customers by combining something the customer knows (username and password), with something the customer has (a credential such as a card, token, or mobile phone).

Banks and credit unions can choose the forms of Symantec VIP authentication that they want to offer customers, Howell explains. Customers can receive soft tokens such as one-time numeric passwords texted to their phones or sent as a voicemail. Or they can use a hard token. "Physical tokens such as a card that receives a numeric code via the Internet play well at community banks, because they're attempting to get market share away from megabanks," says Howell. "They're also interesting for credit unions that are going after those small business customers. It's an opportunity for them to bring in some cash management functionality and cash management security that megabank customers are familiar with."

Protection in reserve

"Let's assume that our authentication technologies have failed," Anderson says. "The end user's PC and perhaps phone are both compromised, and an attacker is in-stream to every bit of data that goes back and forth between the server and the client."

In that case, Anderson adds, "what we do to protect the end user is automatically take two straightforward steps: one, identify compromised accounts based on their behavior, and two, stop transactions that appear to be anomalous or fraudulent. The combination of those steps is what makes them effective." To date, no accounts protected by Symantec VIP have been compromised, Goldwasser says. "Feedback has been very favorable and comments have been centered on how easy it is to use," he reports.

"People want to trust the institution they bank with. When they see the vault, they feel that everything is safe. They need that same type of feeling when they go through the e-channel."

Adam Anderson
Chief Technology Officer
Q2ebanking

The shoemaker wears the shoes

Q2ebanking is also using Symantec VIP internally, because much of its workforce is in the field. "We're as dependent as any other modern enterprise on mobile email and instant messaging over our secure Microsoft-linked messaging platform," Anderson says. "We use Symantec VIP for remote access to our virtual private network (VPN), because part of our disaster recovery and around-the-clock support strategy for our customers relies on our support, implementation, and development staff being mobile."

The company's infrastructure is designed to help employees work from anywhere. "It's been a really effective and productive approach," Anderson adds. "The development staff or anyone else who has access to the production network uses physical tokens. For general use, we offer the software version of the token on a smartphone."

Q2 likes the physical token option for critical access because it can be more easily revoked. "If we had to terminate an employee or an employee will be out for an extended period of time, we're more comfortable collecting the physical token than we are deregistering the mobile software version," Anderson says.

How is Q2ebanking being received? How much do American customers and banks want mobile and online banking that is convenient and secure? Enough to make Q2ebanking among the Inc. 500 fastest growing businesses in America—for two straight years. The rate of growth over three years is 912 percent.* In a down economy, that's a solid achievement.

* inc.com "2011 Inc. 500" Accessed November 4, 2011