Webinar

# Design Your Digital Strategy with an Emphasis on Security

October 2017

Q2's Bob Michaud and David Brebner provide detailed views surrounding the proliferation of personal data, concerns about that data being used against people and organizations, and the need for layered security to deter cybercrime—particularly in the financial industry.

As Bob describes it, the branch network was designed with security as a foundation. Bulletproof glass and security guards helped convince consumers to trust financial institutions. Digital banking is similar, but trust is established and maintained through strategies that deliver transparent security embedded inside the account holder's experience.

### Context

The data available from digital channels can reveal a lot about a person. Shared information from social media can provide a complete picture of account holders' likes and dislikes, profession and workplace, and even their pets' names (a password favorite). Unshared information, such as location-based and other device data, can reveal where people shop or where they park their personal vehicles. Taken in total, this information can be used for good or bad.

Financial institutions must ensure that information is not used against them or their account holders. Layered security can help greatly.

These five layers include multi-factor authentication, transaction-based controls like verification alerts and dual approvals, behavioral-based or anomaly detection that recognizes out-of-the-norm behavior, account activity controls like positive pay, and end-point-centric controls.

# Key Takeaways

The five layers of security discussed in this webinar help build better digital experiences for account holders, and should be part of a financial institution's overall digital experience strategy—not just across customers, but across account and transaction activities.

Not all customers and transactions are created equal. A consumer does not have the same requirements and concerns as a commercial enterprise that needs to make payroll, uses ACH and wire payments, and has multiple employees accessing accounts. To have a balance of security with the need of an account holder, a layered security approach that can be adjusted per case is a proven way to go.

> "What we have to do in the financial services sector is build an experience that leads to digital trust."
>
> — Bob Michaud

## It can be easy for types of traditional authentication factors to be compromised.

Acquiring a list of email addresses off the dark web is a relatively simple task. Consequently, educating people on how to make their passwords more secure and creating unique challenge questions will improve deterrence against hackers and other cybercriminals.

## Until the digital channel makes changes to the use of passwords or challenge questions, we all need to think of security differently.

Simple changes like developing techniques that provide "unique" answers would help secure the digital channel better. For a challenge question – such as "What high school did you attend?" – an answer could be something unrelated. Instead of providing the name of a high school, a pet's name could be used.

"If we know more about them (people), and we can put that in context around security, then we get to a point where a layered security model understanding some of this information can extend security capabilities."

—David Brebner

# Biographies

**Bob Michaud**
EVP & Chief Technology Officer

Bob Michaud is responsible for all Q2 audit, risk, and compliance activities – as well as overseeing the delivery and execution of the company's overall information security strategy. He specializes in risk management and assessment, compliance and regulatory management, product development, disaster recovery, and incident response. Bob's experience in the financial services industry spans 35 years, including 20 years in leadership roles. Prior to joining Q2, Bob was Executive Vice President of Client Operations at Continuity and Head of Audit Risk and Compliance at Fiserv. He earned a bachelor's degree in Finance from the University of Nebraska-Lincoln.

**David Brebner**
Product Owner III

David Brebner has 20 years of domestic and international experience in digital financial services, and has worked in Australia, the U.K., and the U.S. David's focus areas include customer experiences and journeys, and digital banking and payments. His background includes consulting and advising on strategic direction, product management, solution design and implementation, account management, and marketing. With his breadth of experience, David has likely seen a similar problem before and is prepared to tackle any challenges thrown his way. He holds an undergraduate degree in Cartography from the University of South Australia.

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