• • • A CLOSER LOOK

protiviti®
Face the Future with Confidence

Balancing Customer Experience with Security and Fraud Controls

Financial technology firms, widely referred to as fintech companies, are often defined as new entrants to the financial services industry with a focus on the use of innovative technologies aimed at disrupting established processes or customer experiences. The industry is also witnessing the rapid growth of fintech groups created or acquired by larger, established financial institutions.

These groups often have a mandate to either develop their own technology or partner with, invest in, or acquire emerging fintechs. Despite their evident popularity, however, some consumers and regulators alike are concerned about the security and fraud controls the emerging players provide, especially if the start-up companies offering these products have not considered these issues fully from the outset.

Jason Goldberg
Director, Financial Services Business Performance Improvement, Protiviti

Jason Goldberg, a payments industry veteran and a director with Protiviti's payments and retail banking practice, shares his views on how the emergence of fintech firms is impacting the traditional financial services industry. This paper is part of a broader series from Protiviti exploring how new technologies are disrupting financial industries.

How are new fintech products and services affecting the traditional financial services market?

Jason Goldberg: New entrants are focusing on disrupting two main areas of the financial services industry: the first is established network or systems, such as payments, banking, or wealth management, and the second is customer experience.

The new entrants are mostly smaller entities, which are nimble and can implement technology faster than more established players. They think about the customer experience from day one and build their services and products around that premise. This has put pressure on the larger, traditional financial institutions to understand how they can streamline their existing processes to improve the customer experience and remove as much friction as possible between them and the customer.

> *[New entrants] think about the customer experience from day one and build their services and products around that premise.*

This is a significant challenge for them, since many are managing products and systems that are decades old. They have continued to build products on top of products, features on top of features, systems on top of systems, taking a "bolt-on" or repair methodology and mentality to service development. When firms start to bolt on new products or services, or if processes are repaired to improve servicing, very few are structured to consider the implications for the end-to-end customer experience, which has a significant impact on the overall customer experience.

Can you give some examples of innovations that have improved the customer experience?

Goldberg: The drastically increasing use of biometrics for authentication has been a major market differentiator. Apple was one of the first companies to adopt biometrics for iPhone users to unlock their phones, and now more and more app developers, including the vast majority of major financial services firms, now enable their apps to be unlocked, or enable the customer to be authenticated, using that same biometric technology.

This technology is incredibly simple, but it has a tremendous impact on the customer experience. As banking moves increasingly onto mobile devices, such a significant shift requires buy-in from all departments within the institution, including product design, marketing, risk and compliance, security, regulatory, and IT.

Another example of biometric authentication is voice recognition. One such system has been launched by a major U.S. financial institution in partnership with Amazon's Echo product. Bank customers that have Amazon Echo are now able to use their voice to request services such as their account balance, and to schedule bill payments, by calling on Alexa, the Echo's in-device call sign.

Although this is a very forward-looking use of voice authentication technology, most financial institutions are unlikely to copy such functionality, primarily because of security and privacy concerns. With fingerprint biometric authentication, users can unlock and read information on their screens, but voice responses on Echo would be broadcast to everyone present in the same room, or within earshot. That being said, it is refreshing to see larger financial institutions continuing to test and trial new technologies even amid the existing regulatory landscape.

As banking moves increasingly onto mobile devices, such a significant shift requires buy-in from all departments within the institution, including product design, marketing, risk and compliance, security, regulatory, and IT.

New entrants are significantly improving the customer experience in the person-to-person (P2P) payments sector. Innovators such as Venmo and Mobeewave have done a terrific job of allowing the customer to transfer money from one person to another with very little friction, using just one or two clicks. A traditional banking app often requires further authentication and takes more clicks to make a deeper dive into the app. This sort of innovation is driving the traditional players to work to reduce the number of pages and the number of clicks, something they are very used to working on through voice-response units (VRUs) or web channels but that has now moved to growing channels such as mobile and in-vehicle telematics.

How are new entrants dealing with security and privacy requirements?

Goldberg: Many new entrants do not have the same level of focus on security, fraud and privacy that the more traditional players in financial services have, and must have, because of regulatory requirements and scrutiny. Simply put, the larger players have all come under scrutiny before and have more to lose. Some new entrants probably need to have a deeper focus on security and privacy; not least because it is only a matter of time before they, too, are regulated more closely.

New entrants risk falling into the same bolt-on trap as their larger competitors. In this case, they may later find themselves having to bolt on security and privacy controls, which will inevitably impact their customer experiences. This is precisely what slowed down the traditional players. It makes more sense for some of the new entrants to include robust security controls and regulatory compliance at the design stage.

However, in my experience, security and privacy controls tend to be an afterthought. New entrants have a very different mindset from that of the traditional financial institutions. They are thrilled to have a customer experience that is better than that of the established players, but they need to be mindful that success brings greater regulatory attention.

A good example of this is Dwolla, the online funds transfer platform that provides its services to banks and other institutions in an application programming interface (API) format, with an incredibly streamlined customer experience. Because the company grew so quickly, regulators began to look at some of its security promises. The Consumer Financial Protection Bureau (CFPB) fined Dwolla $100,000 in March 2016 for deceiving consumers about its data security practices and the safety of its online payment system.[1]

Contrary to Dwolla's claims, the CFPB found that the company failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access, that it did not encrypt some sensitive consumer personal information and that it released applications to the public before testing whether they were secure. The company agreed to pay the fine and fix its security practices. While the value of the fine was not significant, it was the overture for other emerging entrants to be more mindful of their practices.

Success for new entrants brings with it the challenges and requirements that some of the existing institutions are facing. The larger players are now figuring out how they must respond to these challenges to become as nimble as a new entrant but still meet their regulatory and customer requirements.

What should traditional financial institutions be doing to assess and counter the threat from new entrants?

Goldberg: Traditional financial services firms need to think about embedding security, fraud, risk and compliance requirements and controls at the very earliest stages of the innovation and development processes. Many firms, including the successful new entrants, approach this development from a bolt-on standpoint: Create the innovative new product first and only then pull in fraud, risk, security and privacy controls. That is absolutely the wrong approach.

> *New entrants have developed a culture where everyone sits openly and works together fluidly – albeit often without the strong focus on security and regulatory compliance.*

During the design stage, the innovators, the designers, and IT experts all need to be in the same room with individuals from security, privacy, fraud, risk and compliance. Individuals from the more traditional control areas of the firm need to have a developmental mindset and consider the customer experience as well as the control environment as partners in the innovation and development cycle, rather than being viewed as a team that comes in to stunt growth.

This is a key cultural difference between new entrants and traditional players. New entrants have developed a culture where everyone sits openly and works together fluidly – albeit often without the strong focus on security and regulatory compliance. In many traditional financial institutions, these functions are somewhat siloed.

Very often, the IT department is engaged on a project only once specific requirements have passed the concept stage. Functions such as risk, compliance and security tend to have a somewhat adversarial relationship with the front-end product, marketing and innovation teams within these firms. This is a major problem and a major weakness for the traditional players. Traditional firms need to find people from within those functions that have expertise in both risk and security, combined with an innovation mind-set. Too often, however, the perception is that they are working to stifle innovation rather than lead it.

[1] Consent Order, Consumer Financial Protection Bureau, Mar. 2, 2016: http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.

How can firms balance the customer experience with security and privacy?

Goldberg: Firms need to approach the development of new products and solutions using a customer lens by creating customer-journey maps. Such maps should be created for each customer persona, and for each target segment, to examine every customer touchpoint. This process helps firms better understand how to balance the customer experience with security and fraud controls to apply the appropriate level of friction between the touchpoints, using intelligence, analytics and data to drive down some of the customer-managed security and fraud controls. Success requires achieving balance between a positive customer experience, appropriate level of customer friction, and back-end controls using cutting-edge security and fraud tools that are invisible to the customer.

Part of the challenge is around customer perception. Adoption of new technologies begins with specific demographic segments and then spreads. The early adopters often inherently trust the security in a new product or service offered to them. The new entrants have exploited this, providing perceived security in place of robust controls. Larger firms would be well served to exploit the vulnerabilities of their emerging counterparts.

The large banks know that these threats exist. Anthony Jenkins, former CEO of Barclays, recently predicted an Uber moment for banking. He is spot on. There is going to be a massive disruption on both sides. Jamie Dimon, CEO of JPMorgan Chase, conceded that although his bank's customer experience is not as strong as those available thanks to some new entrants' products and services, Chase can offer proven security and stability, especially during a downturn. Although this issue is separate from the customer experience, his is an interesting comment that shows his perception that customers will choose the security and stability of a larger institution over a cool app, especially in trying financial times.

Contacts

Ed Page
Managing Director
+1.312.476.6093
ed.page@protiviti.com

Tyrone Canaday
Managing Director
+1.212.603.5435
tyrone.canaday@protiviti.com

Atul Garg
Managing Director
+1.704.972.9612
atul.garg@protiviti.com

Jason Goldberg
Director
+1.212.471.9678
jason.goldberg@protiviti.com