2016 Accenture Technology Vision for Banking

Digital Trust: Erase the trust paradox in banking

High performance. Delivered.
Under the theme “People First: The Primacy of People in a Digital Age,” the 2016 Accenture Technology Vision highlights five emerging technology trends shaping the new business landscape: Platform Economy, Digital Trust, Liquid Workforce, Intelligent Automation and Predictable Disruption.

This report offers a banking industry perspective on Digital Trust. Banks will need to address each trend first from a strategic business and then a digital enablement lens as they begin to transform themselves Beyond the Everyday Bank, interacting daily with customers to meet their financial and non-financial needs every day.
Banks' digital trust paradox is becoming unsustainable

In financial services, digital trust is central to the customer relationship. Eighty-four percent of bank respondents to the Accenture Technology Vision 2016 Survey agreed that trust is the cornerstone of the digital economy.

Banks are one of two company types, along with telcos, that consumers most trust with their personal data, according to Accenture research. In North America, 86 percent of consumers trust their bank over all other institutions to securely manage their personal data. This is not surprising given that banks have had access to a wide range of consumers’ personal information for quite some time and have gradually built a high level of trust. Transactional trust remains high, even as consumers recognize that banks are primary targets of data hacks.

While customer transactional trust is an advantage for banks, customer relationship trust is not. Customers rank financial services companies among the least trusted in terms of being relied on to behave in ethical ways, according to the 2015 Edelman Trust Barometer report; 45 percent of informed respondents in the U.S. say there is not enough regulation of the Financial Services industry. Due to scars from the industry’s past scandals and questionable conduct, customers are reluctant to trust banks as advisors.

This customer trust paradox is growing ever volatile in the digital age, heightening participants’ sensitivity and exposure to risk. The more customers trust banks with their digital transactions, the more banks roll out digital services. In the US, for example, JPMorgan, Wells Fargo and Bank of America grew their mobile customer base by a collective 71 percent, to 57.7 million over the past three years. It’s a dynamic cycle which makes customer data increasingly vulnerable. Banks continue working to secure data, such as introducing biometrics to validate mobile banking transactions, which most often gives customers access to multiple, if not all, of their financial accounts through one source. If compromised, it opens a door to more customer information. Add to the risk the fast-increasing number of mobile apps that consumers link to their financial information and the fact that financial settlements pass through various aggregators and intermediaries. Nearly 80 percent of bankers strongly agree that they are exposed to more risks than they are equipped to handle as a digital business. Eighty-five percent say that as data-centric products and services put data-handling concerns in the spotlight, companies are exposed to exponentially more risk; and 85 percent agree that a lack of security and ethical controls on data could exclude them from participating in other companies’ digital platforms and broader ecosystems.

At a time when banks struggle to find additional revenue, a massive amount of data is available to collect, manage, secure and, possibly, monetize. More than 80 percent of bankers agree that data is evolving from being a valuable resource to becoming the basis for entire business models. The question, then, is how can banks better use data and digital technologies to enhance safety of traditional banking and grow relationship trust?

84% of bank respondents to the Accenture Technology Vision 2016 Survey agreed that trust is the cornerstone of the digital economy.
(Re)build bank customers' confidence

The digital opportunity for banks is two-fold: extending customer data to act for the customer's good while also making money from data, such as through behavior-based tailored selling or more profitable existing services. Banks that capture the opportunity will go beyond regulatory compliance to act in ethical ways that protect and grow customer relational trust.

Banks already comply with Know Your Customer regulatory standards and thus have a goldmine of data ready to yield business value. For example, identity data on a teen saver can signal a tailored credit card offer when the teen enters college. Projected further out, that teen-turned-adult may be ready for a mortgage, investment planning or a business loan. Data analytics can help banks sense customers' “seasons of life” events to offer personalized products and services at the right time to engage customers and deepen their trust. As an added benefit, what other providers might value such predictive insight?

Another opportunity for banks to rebuild trust is through opening windows to their digital footprint in the personal advisory space. Employing digital stamps, for example, will give customers the transparency to better understand and follow the advisory process, and collaborate with banks toward intended outcomes. Banks, then, welcome customers to hold them accountable which, in turn, increases customers' comfort and trust levels at lower cost. The process is not just compliant, but value-adding.

Of course, such trust-building strategies mean reassuring customers on data privacy and transparency. In doing so, banks can take ethical guidance from customers on what matters to them. For example, banks could simply ask customers about their ethical thresholds; what do they see as the boundaries? How might the boundaries shift at various and specific value situations? Of course, different customers will have different ethical tolerances and contexts. Still, it should give banks a strong perspective on the balance between data value and moral limits for key transactions—enough to turn data and digital operations, ethically and legally, into revenue.
Fostering a culture of ethics requires banks to take decisive actions in key areas, such as how best to:

- **Communicate clearly to consumers on customer data being collected, for what purposes, who can access it legally and how it will be used.** If, for example, a bank determines from social media that a customer engages in high-risk behavior, such as skydiving, should the bank consider this insight in assessing the customer’s credit risk?

- **Use data primarily to offer customers reciprocal benefits that are directly relevant to the data and service being provided.** Only 28 percent of consumers Accenture polled are willing to share additional personal data if that information is then going to be shared with a third party, highlighting the importance of the data control dimension of digital trust.

- **Be responsible to accurately collect, manage and access customer information, with accountability for the use of data.** Eighty-three percent of banks see a strong or very strong demand for increased ethical controls of data among their knowledge workers.

Banks are working to improve their digital ethics. For example, Barclays is building digital trust is through its Digital Eagles program, which has trained more than 12,000 employee volunteers to directly provide support to customers, consumers and business owners in branches and in nearby community locations on how to get online, build digital skills and benefit from digital use—whether related to Barclays products or not, and sometimes with complimentary tea.
Combine ethics with security
Security plays a significant role in the pursuit of envious customer trust and data-driven revenue.

Given the pace and scale of Big Data and IoT, it is growing more difficult for banks to prevent cyber attacks. Nearly 70 percent of banks suffered from at least twice as many (or more) privacy or security breaches compared to two years ago. According to a Bank of England report, 46 percent of banks polled in the second half of 2015 cite cyber risk as a key concern—compared to 30 percent in the first half of 2015 and 10 percent in the last half of 2014.7 According to a global insurer, cyber attacks cost businesses as much as $400 billion a year, including the initial damage as well as ongoing disruption.8 Then, 54 percent of digital consumers are cautious about the information they share due to lack of confidence in the online security that protects their personal data, according to Accenture research.9

To give customers and ecosystem partners the data security they want and need, banks must begin to require above-and-beyond measures in their operations. They will need to adopt a data-centric philosophy, knowing the IT structures and data that are valuable and need protecting in certain ways. It means strengthening bank security strategies toward higher digital trust, such as:

- **Adopting a zero-tolerance approach**, along with a cyber-risk appetite, in operating more digitally and participating in digital ecosystems with open platforms that share data and transactions.
- **Incorporating next-generation security mechanisms** in managing data security risks. Technologies, such as “follow data wherever it goes,” is helping in this area.
- **Rethinking identity and access management**, using more innovative techniques. For example, InAuth is a mobile-device security company that establishes the trustworthiness of a device before granting it access to network resources. Once a device is validated, solutions from the likes of BioCatch employ multifactor authentication that considers the way users interact with devices as a way to verify and provide persistent identity. According to BioCatch, more than 33 million banking customers around the world are protected with its behavioral biometric technology.10
- **Integrating security solutions**—such as security-aware application design, integrated database security, dynamic access controls, and runtime application protection—into new products.
- **Identifying indicators of risky insider activity**, putting in place internal components—such as Next-generation electronic communications surveillance—to detect early signs of possible fraud or criminal activity, whether intentional or unintentional. The world’s biggest banks could boost their earnings by as much as $500 million a year by reducing their misconduct penalties by just 10 percent.11

Banks are being proactive to strengthen authentications and IT security by incorporating biometrics as a game changer. For example, USAA is one of the first banks in the US to allow customers to log into their account over their smartphone using their face, fingerprint or voice for identification purposes.12 Mastercard is looking to launch a new contactless card with an embedded fingerprint sensor as a more secure transaction method; HSBC bolstering its security procedures with voice and touch recognition security services in the UK to reduce customer passwords and memorable questions requirements; and Barclays is offering fingerprint scanning for authentication of large transactions.13

Putting in place structures, technology and processes to engage digital ethics with security is critical for banks to compete today. What was once a discussion simply around IT security is now a much broader responsibility for all bank stakeholders to ensure high levels of digital trust and new revenue opportunities.
Digital Trust:
100-Day Plan

Over the next three months, banks should understand the current state of digital risk and data opportunities before them, and look for ways to create value.

1. Assess tolerance for trust and data security risk, both your own and that of your ecosystem participants. How much risk are you willing to absorb, and does this match your Board’s expectation?

2. Survey stakeholders and tap sources of ‘trust’ insight (e.g., customer service logs) to quantify the level of trust and ethical appetite across your business portfolio.

3. Create an Ethical Value Proposition, answering fundamental questions of purpose, value creation, impact on operations and possible engagement with customers on the right approach.

4. Take an inventory of data-driven business processes; describe the current and potential opportunities for enhanced security and data ethics for each.

5. Identify the executive(s) responsible for building and maintaining trust, digital ethics, and security with vendors, partners, and customers.

6. Partner with an academic institution, non-profit, or industry group to dive deeper into one aspect of digital ethics. Publish findings/advice for others.

7. Compile a list of opportunities to bring additional security to data.
About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

Made by Accenture Research

Accenture Research is a global team of industry and digital analysts who create data-driven insights to identify disruptors, opportunities and risks for Accenture and its clients. Using innovative business research techniques such as economic value modeling, analytics, crowdsourcing, expert networks, surveys, data visualization and research with academic and business partners they create hundreds of points of views published by Accenture every year.

Follow Accenture Banking

LinkedIn Accenture Banking
Twitter @BankingInsights

The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, these ideas should not be viewed as professional advice with respect to your business.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, these ideas should not be viewed as professional advice with respect to your business.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

Copyright © 2016 Accenture
All rights reserved.

Accenture, its logo, and
High Performance Delivered
are trademarks of Accenture.