KPMG Perspectives

Can analytics build trusted customer relationships in banking?

Technology, new business models and trust

THE connection between trust and analytics is well understood within the tech sector—consider the opportunities and challenges associated with autonomous vehicles, for example. There is something similar taking place in the banking sector as it continues to struggle with issues of trust. According to Edelman's 2016 Trust Barometer, consumers now trust technology companies far more than banks. While Edelman's rankings show some improvement in trust for financial-services organizations over the past few years, the industry still ranks last, behind the pharmaceutical industry.

So how does a customer trust a bank to do the right thing? How does a bank trust its employees to do the right thing for the bank and for its customers? How do board members know they can trust the information in front of them? Some specific data challenges are already front-of-mind in banking, such as cyber security and data protection.

New technologies, such as blockchain distributed ledger technology, have enormous potential to transform the sector using a fundamentally different mechanism to help assure trust. However, there are wider risks and opportunities as analytics take on more decision-making functions. In the future, analytics of various types will play a central role in multiple relationships of trust in banking—between board, shareholders and staff, between customers and brand, between regulators and the sector as a whole.

Let's take two trends as examples. The first is the rapid growth in the financial-technology (fintech) sector. Fintech and digital upstarts recognize the tremendous opportunity analytics bring and have benefited from the trust gap between banks and their customers. In fact, we believe one of the biggest reasons that fintech companies have been so disruptive to banks is that they leverage an inherent consumer trust in technology with offers of convenience and innovation in a sector that has largely been starved of new models for decades.

In the European Union the trust gap is being formalized in a dramatic structural change in the market for payment services. The revised Directive on Payment Services (PSD2) will pave the way for third-party direct access to bank accounts. The quintessential element of this provision is that banks will have the obligation to grant access to payment data to other parties (nonbanks), which may marginalize traditional banking business models. This puts banking at the center of a perfect storm. The new, tech-driven players create a promise of greater trustworthiness, as well as a better user experience.

Traditional banks are now competing furiously. As the new fintech organizations and nontraditional disruptors clearly demonstrate, advanced analytics can be harnessed to predict customers' needs and demands effectively. Prove that you know your customer and understand their needs and you can quickly build trust relationships, especially among the emerging group of millennials who likely lack any ingrained attachment to more traditional methods of banking.

In parallel, a second trend that is bringing analytics and trust closer together—is the rapid development of risk analytics, which is creating new trust issues. Risk analytics are relatively mature, with widespread use in the prediction and evaluation of employee conduct, fraud and risk exposure. Predictive analytics for employee conduct are closely associated with building consumer trust and have been highly effective at identifying and reducing unethical behavior. However, the area of "conduct analytics" is one in which we find increasing concerns about breach of trust between bank and employee, as too much intrusion can overstep the "creepy line" and the wrong conclusions can damage reputation.

More generally, the stakes are rising. Predictive risk analytics have been shown to work well for common everyday risks, but are still largely untested on rarer colossal risks. If there is no clear history of events or agreed future scenarios which can act as a baseline for automated risk assessment, then it is easy for trust to be misplaced in complex but untested mathematics, as demonstrated by the failure to predict critical market risks during the 2008 global financial crisis.

Do you trust the analytics?

WITH analytics playing an increasingly powerful role, the potential consequences of errors and underperformance increase. But we believe trusted analytics need to demonstrate more than basic good practice in solution development and data management. Indeed, just as banks need their employees to act with integrity, they also need their decision engines and algorithms to act with integrity. In fact, maybe more so: an unintended bias coded into an algorithm will spread rapidly until it is found and fixed, which could lead to significant issues of mistrust between banks and customers.

Already, we seem to be moving to a point where we, as consumers, are gradually becoming more comfortable with robots performing various high-level activities and

tasks than we may be with people. The new market in "bots" looks likely to take on simple customer services. Employees, boards and customers increasingly trust decision engines and algorithms with important and often material decisions. Robo-advisors are increasingly chosen to guide both individual investors and their advisors. And a surprisingly large number of consumers seem to place trust in the offers they receive.

In many of today's banks, analytics influence so many touch points and decisions that algorithms and decision engines are becoming a new type of agent, constantly working on behalf of the organization, integrated into virtually every aspect of the sales cycle and owning key parts of the customer relationship.

The issue is that only a few banks currently give as much attention to the integrity of their analytics as they do to the integrity of their employees. Analytics are typically treated as a "black box," whereas, in reality, organizations need to start thinking about their analytics as independent entities unto themselves; as critical intermediaries between the stakeholders and the organization.

This creates new challenges for banks and their boards, who are essentially being asked to hand over the decision-making reigns to a third-party "entity" that a bank may or may not have fully understood.

Applying a trusted analytics framework

FOR bank boards and executives, the question of what to do with such a wide range of potential risks and opportunities ultimately needs to start where analytics can protect or destroy the greatest value. For these areas, banks should ask themselves on what basis they trust their analytics. And who is the judge?

Banks and their regulators need to have the proper frameworks in place to be able to trust the data and analytics that underpin their decisions and actions. As we proposed in the series' first article, "The Power of Trust in Analytics," help assure trusted analytics across an enterprise can be addressed across four key dimensions, or anchors: quality, effectiveness, integrity and operational control. Our experience suggests that it will take a consistent focus on all four anchors for banks to achieve a higher level of trust in their analytics.

Quality: Are the underlying data and the analytics of high quality?

MOST banks are aware of the need for fresh and reliable data and the significant challenges this creates for "know-your-customer" (KYC) programs, for example—new questions arise as analytics fulfills a greater role in the organization. Is the right mathematical model being applied? And how do you maintain data and analytical quality when working with a wide range of providers and internal talent? What capabilities, processes and controls should surround analytics in different business functions?

Effectiveness: Does it work as intended?

EXECUTIVES and regulators want to be sure that the analytics not only work in theory, but also in practice, that they achieve their intended purpose in the context in which they operate at any given time. This is not always easy.

As machine learning and artificial intelligence (AI) applications spread to increasingly complex real-world systems, we may not be certain during development whether a specific use of data will work in real life or whether a model trained on historical data will be a fair reflection of future reality.

This issue applies to a wide range of predictive analytics and decision engines, from client prospecting and micro-targeting to fraud detection and market risk management. For example, when using analytics to predict mortgage defaults or risk coverage, managers will want to be sure they are using an approach that is right in that specific context.

In some cases, the consequences of sub-optimal effectiveness are likely to be no more than missed opportunity, although this could become a significant cost as algorithms influence an increasing proportion of revenue. In other cases, algorithms can carry major unintended risks, such as market volatility or failure.

Banks need to ensure that they are using the right analytics (as determined by experts in the field) to achieve their intended outcome in each situation. They will also need to ensure employees are using the analytics in an appropriate way: hijacking an algorithm (or taking it off the system) for personal gain, for example, would pose a significant risk for banks.

Integrity: Is its use considered acceptable?

LEGAL compliance—for example, with data-privacy laws—is only part of the story. In many ways, an extension of the conduct debate, a clear framework for integrity, increases the chances that the analytics are being used in the best interest of the consumer and will be key to creating trusted analytics.

Not all enterprises will want to follow the same ethics strategy. Beyond a minimal compliance-only approach, there are options to take a specific, risk-focused approach or a more transparent values-based approach as part of a wider brand strategy, for example.

Banks need to understand the implicit deal they have with their customers and will need to be careful not to overstep the bounds agreed in the relationship. Just because you have the data and can do something legally, does not always mean that you should. For example, too much intrusion can overstep the creepy line with customers.

Operational control: Is long-term operation optimized?

IN a fast-changing, data-driven world, the management of analytics never stays still. Banks are familiar with cyber vigilance, technical progress and changing regulations, but are less accustomed to issues of data currency and algorithm "lag," where (overtime) analytics can perform differently and lag behind best current practice in human decision-making. Banks need clear governance strategies—not only for emerging risks, but also to optimize performance and justify investments.

The article was taken from KPMG's publication, entitled *Can analytics build trusted customer relationships in banking?* by John Hall of KPMG in the UK and Mitch Siegel of KPMG in the US.