Deloitte.

FINANCIAL SERVICES INDUSTRY
MAY 2023

Digital ethics and banking: A strong AI strategy starts with customer trust

Contents

In today's fast-paced financial sector, data is an invaluable tool – allowing banks and financial institutions to spot imminent financial trends, identify emerging customer needs, and roll out customized services and offerings in record time.

With artificial intelligence (AI) now entering the playing field, data-led banking is evolving even more rapidly. Yet, to lead this technology in the right direction and enhance responsible implementations, trust is essential.

A key pillar in building that trust involves creating trustworthy technology, or digital ethics. Beyond protecting the rights of users, an ethical framework helps to prevent harm and secure the trust of the people subjected to technologies such as AI models. Failing to take digital ethics into account, on the other hand, can result in the creation of solutions that ignore the needs of underrepresented groups or that can be used in ways disconnected from organizational intentions.

This latter path can further interfere with organizational goals, tarnish brand reputations, and even negatively impact peoples' lives. To avoid these outcomes, financial institutions must take a new approach to data in the AI era by putting trust at the center of all their decision-making. This means reframing their mindsets, enhancing awareness of existing systemic shortcomings, and having meaningful conversations around ethical data collection and management.

Here, we explore some of the barriers banks may encounter as they integrate AI into their data-led banking practices, as well as solutions to overcome them by integrating ethics throughout business practices.

Common challenges

In an ideal world, AI algorithms should help financial institutions acquire the insights they need to make informed business decisions and roll out products and services aligned to their customers' needs in a responsible way.

Unfortunately, it doesn't always play out this way. Some of the common challenges banks encounter include:

Customer resistance. To support their customers' financial health and drive loyalty and satisfaction, financial institutions require personal data. This data can be used to create better products and services, which ultimately help customers gain more actionable insights into their existing financial situations and achieve their financial goals. In many cases, however, customers remain hesitant to share their personal data. This may be because they don't trust their financial institutions, don't understand the benefits of sharing this information, or feel forced into providing personal data. Some people feel uneasy having their information codified and would prefer to have a choice in whether their data is collected by an institution.

Human bias. Whether conscious or not, all human beings carry biases—and these biases make their way into AI algorithms. This can result in skewed data and lead to products that not only fail to meet the needs of financial consumers, but unintentionally result in unfair outcomes as well. For instance, most banks collect data from banked customers (those who meet certain income thresholds) and tailor their financial products based on this information. These thresholds often exclude underbanked customers, preventing them from gaining access to tailored products that could help them enhance their financial position.

Grey areas. When collecting data, it can be challenging to balance business objectives, societal expectations, and duty of care. After all, only a few things in this area are actually black and white. For example, imagine a financial institution that is gathering information about a client to determine whether a financial product is right for them. As they dive deeper into the client's broader financial situation, they discover the client has a gambling addiction. How should they act on this knowledge? Do they have a responsibility to intervene? Questions like these are complex and require a digital ethics strategy that is based on organizational founding norms and values.

These are just a few examples of the complexities that arise when attempting to integrate AI into data collection and management practices in a trustworthy way.

The trust factor

One way to overcome these challenges is to place customer trust at the center of your data strategy.

This will likely involve focusing on three key areas:

1. **Data transparency.** Customers are more likely to share their data when they understand how that data will be used, why sharing it is important, and how it will ultimately benefit them. Specifically, it's important to show customers that the benefits to them outweigh the benefits to the financial institution. Creating this perception requires a strong communications strategy – one that clearly explains the role and purpose of data and seeks to build customer trust. It also means prioritizing "trustworthy AI" – AI that is fair and impartial, robust and reliable, safe and secure, responsible and accountable, transparent and explainable, and preserves privacy.

   One way to enhance transparency in general is to abide by guiding principles, like those set out by relevant national or industry bodies. These principles are designed to help financial institutions navigate this new terrain as it unfolds and implement AI that is not only transparent, but also fair, ethical, and accountable every step of the way.

2. **Customer autonomy.** While privacy regulations and standards provide valuable guidance around ethical AI design, a sure-fire way to build customer trust is to go beyond the bare minimum and offer customers additional control over their data. For example, financial institutions can give customers the opportunity to opt in or opt out of data sharing – or they can allow customers to choose their preferred level of personalization when receiving financial advice on the banking platform. Essentially, the point is to give customers a greater sense of autonomy and allow them to freely choose which kind of data they would like to share, rather than having it taken from them. By taking this route, and earning customer trust, institutions will have more of a license to use customer data to build new digital solutions.

3. **Brand trustworthiness.** While building customer trust around your AI and data collection practices is important, these efforts won't be worth much without a trustworthy brand. At a time when less than half of customers trust banks to do what is right – and financial institutions are under fire for things like greenwashing – those willing to make a conscious effort to build a trustworthy brand will be able to differentiate themselves from their competitors and inspire customers to share their data. This can involve taking a stronger stance on social or environmental issues, or even demonstrating how customer data has led to better products and supported people in exciting new ways.

AI for good

This new era of data and AI comes with great responsibility.

To leverage these technologies effectively – and ultimately reduce costs – financial institutions must acquire permission to collect and analyze user data.

The first step in this journey, therefore, is to secure customer trust by building AI models responsibly, acting consciously, and demonstrating that user data is being handled carefully.

This comes with an ancillary benefit as well because transparent, trustworthy AI and data collection practices also benefit society as a whole. When customers can confidently share their data, businesses can build solutions that are more robust, leading to industry advancements that can create more equitable societies and enhance the greater good. This, in turn, earns more goodwill for the organization – resulting in a better society and a win-win for everyone.

If you'd like to learn more about what it takes to act ethically in the age of AI and set a fair and transparent foundation on which to build your data collection and management practices, contact us.

Connect with us

Nick Seaver
Partner – Deloitte UK
Cyber and Strategic Risk

nseaver@deloitte.co.uk

Gerry Kian Woon Chng
Partner – Deloitte Singapore
Cyber and Strategic Risk

gchng@deloitte.com

Annika Sponselee
Partner – Deloitte Netherlands
Cyber and Strategic Risk

ASponselee@deloitte.nl

Malene Fagerberg
Partner – Deloitte Denmark
Cyber and Strategic Risk

mfagerberg@deloitte.dk

Hilary Richters
Director – Deloitte Netherlands
Cyber and Strategic Risk

HRichters@deloitte.nl

J30917