# Responding to opportunities and risks in a changing data landscape

Bank Governance Leadership Network

August 2018

tapestry NETWORKS

EY Building a better working world

# Responding to opportunities and risks in a changing data landscape

> *"People say data is the new oil, but I like to say data is the new uranium. It's extremely powerful, but it can be very dangerous because it can be used in ways we don't intend."*
> — Participant

The conventional wisdom is that data is one of the most valuable assets companies have, with some commenters referring to it as "the new oil." Technology companies have reshaped the global economy by using data and technological innovation to drive their products and services. Banks sitting on mountains of data are realizing the enormous potential in the information that they maintain—and they are in the early stages of generating value from that data. Firms are already experiencing success using data to better serve their customers, improve efficiency across their organizations, improve risk management and monitoring, bring new and innovative products to market, and drive revenue growth.

However, even as banks are racing to collect more data and use it in new ways, technical obstacles, privacy concerns, and regulatory demands are limiting their ability to do so. Meanwhile, third-party access to that data is expanding through things like Open Banking and application programming interfaces (API). The increasing public attention on privacy and data use also raises fundamental questions about different kinds of data and their relative value, risks and liabilities, and ethical uses, as well as questions as to who ultimately owns the data. Banking leaders are now realizing that their firms will require a more strategic approach if they are going to fully capture the value of data while avoiding potential risks and pitfalls. A director said, *"In the past we have not been strategic enough in how we think about or talk about data at all, I don't think any bank has."*

On June 7, 2018 (New York), and June 13, 2018 (London), BGLN participants met to discuss the emerging risks and opportunities around data in banking. In London, participants were joined by Open Banking Implementation Trustee and EY's Global Fintech Leader, Imran Gulamhuseinwala. Drawing on discussions from both meetings, as well as conversations with network participants in preparation for and immediately following those meetings, this *ViewPoints* synthesizes the key themes that emerged:

- Data presents banks with opportunities for growth and efficiency
- Banks must adapt to evolving privacy expectations and regulations
- Access to bank data is expanding
- Data opportunities and risks require a strategic approach to data management and governance

## Data presents banks with opportunities for growth and efficiency

Data is the driving force behind the modern digital economy. More data has been created during the last two years than during the previous 5,000 years of human history.[1] By 2020, one prediction says that about 1.7 megabytes of new data will be created per second for every human being on the planet.[2] Marketing companies now maintain approximately 1,500 data points on about 96% of US citizens.[3]

*"We've squeezed all the value we can out of our capital, so now we're sitting here with this huge data asset and starting to think about how we can get more value out of that asset."*

– Director

Technology giants in Silicon Valley have thrived by using data to uncover patterns and predict customer behavior, thereby enabling them to offer a more contextualized experience and stay on the cutting-edge of their industries. These firms have also had success monetizing their data in other ways, such as by selling it for marketing purposes. That's one reason Facebook and Google alone will account for a projected 57% of digital advertising spending in the United States during 2018.[4] In financial services, nimble fintechs—largely unencumbered by slow-moving bureaucratic structures, legacy, product-centric platforms, and stringent regulations—have shown a similar ability to use technology to leverage data and interact with bank customers in new ways. The resulting competitive environment is pressuring bank leaders to determine how they can effectively leverage their data for a broad range of business objectives.

### Data-driven opportunities are emerging

Like Amazon, Facebook, and Google, financial institutions have lots of information available. The largest banks have massive stores of data—as much as 100 petabytes each—estimated at approximately 25% of the amount of data Facebook has. But after decades of data collection, banks are still in the early stages of effectively incorporating and utilizing the information they maintain. *"We've squeezed all the value we can out of our capital, so now we're sitting here with this huge data asset and starting to think about how we can get* *more value out of that asset,"* said one director. Another participant asserted, *"The role of banks is to be an intermediary to commerce. They must find a role to add value through their data. There is a major retailer that sends data to Mastercard every day. Mastercard has a team of data scientists that can look at it and offer insights. That should be a great place for a bank to operate, but they're are not doing that."*

As they work to outpace the competition, financial institutions are increasingly looking to data to drive revenue growth, increase operational efficiency, and improve risk management and monitoring. *"In a lot of ways, many banks are in the early stages of a transition into becoming information technology companies. Some already refer to themselves as tech firms, full stop,"* said one director. Data can help banks to:

- **Refine business strategies.** Data can help banks gain a better understanding of market trends and anomalies, influencing broader business strategy. For example, in 2016 JPMorgan shifted strategies and product offerings after analyzing 12.4 billion debit and credit card transactions and finding a decrease in everyday consumer spending over the previous two years.[5]

*"Banks must help customers where they are, not expect customers to come to them."*

– Participant

- **Target products and services.** Services can be tailored for individual customer needs and preferences. In early 2018, Citi announced a new app in response to a company-sponsored survey that found 79% of customers prefer to use a single app to manage their finances and 87% want a snapshot of their entire financial life in one place.[6] Seeing how current customers operate across different accounts and business lines enables more cross-selling opportunities. Firms can also gather external data—from the internet, social media, apps, and other sources—to gain additional information, such as who is searching for a new car or home. Looking across a variety of data sources enables firms to develop better strategies for winning back old customers or targeting new ones. A participant suggested banks need to be more affective in using data to tailor how they serve customers: *"How data gets used to drive products is an important question. Banks must help customers where they are, not expect customers to come to them."*
- **Predict and prevent fraud.** Banks can use new technologies to monitor transactions on a massive scale, improving fraud detection, reducing false-positive rates, and enhancing fraud resolution. In early 2018, UK-based bank NatWest noted that it had prevented £7 million worth of false payments by using a machine-learning system.[7] Banks like JPMorgan and

HSBC have invested significantly in financial crime systems that incorporate big data analytics.

- **Improve efficiency.** New technologies like process automation, artificial intelligence (AI), and machine learning, often driven or enhanced by data, will continue to transform financial institutions in the coming years. Machines are especially effective at compiling and sifting through enormous swaths of data and interpreting contracts. Data can be used internally for enhancing workforce productivity, identifying talent gaps and redundancies, and automating manual processes. A recent report predicted that, within the next two to three years, machines will be capable of performing approximately 30% of the work currently done at banks.[8]

- **Ensure regulatory compliance.** Big data can help financial institutions build new compliance reports and perform regulatory tasks like stress tests. Stress testing requires banks to aggregate data that is scattered across the institution and other entities. As a result, banks with more updated systems and more accurate data have an advantage when it comes to compliance.

- **Establish new sources of revenue.** Data on bank customers, such as spending habits, has obvious value to outside companies, even if it is anonymized and unidentifiable. Identifying the value of specific data to potential clients remains a challenge, however. A participant explained, *"The value of data is based on use. … If I just bought an airline ticket somewhere, that might be worth one amount to Marriott, but it's worth a lot less to McDonald's."*

*"The value of data is based on use. … If I just bought an airline ticket somewhere, that might be worth one amount to Marriott, but it's worth a lot less to McDonald's."*

– Participant

## Blockchain continues to inspire debate

Blockchain has often been cited as a technology that may enable banks to use data for exciting new purposes. Though stories of blockchain applications and use cases garner media headlines, current examples of distributed ledger technology applications at scale remain limited. Participants shared a range of views about the potential for the technology in banking.

## Blockchain continues to inspire debate *contd.*

A participant said, *"There is no question it's incredibly overhyped and there are misunderstandings about the technology and what it can do. There haven't been many clear examples of why blockchain is advantageous in a private or closed blockchain environment."* An executive agreed, calling the technology, *"costly, inefficient, and ineffective."* However, other participants remain encouraged about the potential uses of distributed ledger technology to increase efficiency in specific processes or businesses. Some institutions have found success in applying the technology to areas such as trade settlement, international payments, KYC, customer document storage and exchange, and asset and liability management. A director said, *"There are clear examples of labor-intensive processes that could be improved with blockchain."*

Internal management conversations around the technology are still maturing as financial institutions experiment. A participant observed, *"Financial services as an industry is putting the most effort and money towards blockchain technology, but it has been slowing down."* Though banks continue to explore the potential for the technology, they are in varying stages of discussing it at the board level. A director explained that it is still early days, *"We're not talking about blockchain at the board level, we're just not. It's still horizon-scanning."*

### Considering new business models

Banks across the globe are making strides when it comes to using data to improve their current operations, but there are also opportunities for firms to truly think differently and explore new operating models using data and technology:

- Industry collaboration. As the big technology companies continue to leverage data and analytics to provide their customers with financial products and services, banks may benefit from collaborating more closely across the industry. A participant said, "There is a tremendous opportunity to look at how firms work together to create new roles for the industry. Banks have proven success with building networks that allow millions of consumers to work with them consistently—that's where banks have to unite." Some participants suggested banks could benefit from collaborating

*"The value of data is the intersection with someone else … networks are where the real value is."*

– Participant

on issues like data-sharing for financial crime purposes or to improve KYC and other customer onboarding efficiencies. A director asked, "Why can't we get away from being scared and working together for opportunities?" However, one executive noted that collaboration is fundamentally difficult for banks: "The challenge we all have at the core of banking is managing customer trust and identity. Now, balancing that with the need to collaborate … those things are not mutually reinforcing." Another participant asserted, however: *"The value of data is the intersection with someone else. Most banks want to do it themselves, but networks are where the real value is."*

- **Protection of data.** Despite the ongoing reputational issues confronting banking, banks may have a particular advantage when it comes to protecting customer data. The Facebook–Cambridge Analytica scandal and other public controversies during the past few years have contributed to a shifting perception of technology companies. Once considered innovative leaders striving for the greater good of all, tech giants like Facebook, Amazon, Apple, Netflix, and Google are increasingly being viewed as potential threats to society.[9] One report found that 59% of consumers trust banks to safeguard their payments more than they trust alternative payment providers, retailers, or telecommunications companies. Just 12% most trust alternative payment providers like Apple, PayPal, and Venmo.[10]

*"I'm convinced there's a place for banks to become data banks in the same way that they are money banks."*

– Participant

This "techlash" may be an opportunity for banks. *"I think the banks are in a very good [position] vis-à-vis customer trust at the moment,"* said one participant. A recent survey found that their primary banks were the leading choice among consumers when asked which company they trust most with their private information (well ahead of Visa, PayPal, Amazon, Apple, Google, and Facebook).[11] As a result, some participants suggested there may be an additional opportunity for banks in managing data and identity. A participant expert said, *"I'm convinced there's a place for banks to become data banks in the same way that they are money banks, where the bank actually becomes that central place that looks after and is responsible for all that customer data. And charges a fee for that service. I'm surprised I don't see much more innovation in that space by the big banks."* Another asked, *"Are we moving into a new world where there is a new service banks can offer around ownership and protection of identity? It could be a win/win."*

# Banks must adapt to evolving privacy expectations and regulations

As firms work to utilize data more effectively, rising public concerns around privacy and shifting regulatory demands are challenging the very idea of data ownership and forcing banks to rethink institutional approaches to data. *"The banks are only just getting around to thinking about data ownership, and that whole environment is changing,"* said a director.

## The environment around data and privacy is evolving

Recent public controversies have brought concerns surrounding the treatment and use of customer data to the forefront. Facebook's very public saga is the result of an investigation's finding that Cambridge Analytica, a consulting firm, had gathered Facebook data and combined data mining tools, data brokerage, and analysis with strategic communication to impact the electoral process.[12] Consumers have become increasingly concerned with how their personal information is being collected, stored, analyzed, and shared by corporations, and governments are considering stronger laws and regulations to empower individual ownership of personal data. One director said, *"There is a reputational risk that is being taken when we use data. Are we doing that with our eyes open? Also, are we fleet-of-foot enough to know that something that is OK today might not be OK tomorrow?"* Given the potential for significant fines and reputational damage associated with a regulatory violation, as well as the implications for the competitive landscape, participants noted that these are key issues driving conversations at the board level.

*"There is a reputational risk that is being taken when we use data. Are we doing that with our eyes open?"*

– Director

### GDPR complicates data governance

Banking regulators regard consumer protection as a vital part of their supervisory responsibilities, and privacy as a critical aspect of that consumer protection. The European Union's (EU's) General Data Protection Regulation (GDPR), which went into effect in May 2018, empowers citizens to control their own data, and there are signs that similar regulations may spread globally. Banking leaders are wary that there could be significant costs if they are not able to address privacy concerns effectively, as the maximum penalty for GDPR violations is 4% of a firm's annual revenue or €20 million, whichever is higher.[13] The direct fines are a concern, but one participant said the legal and reputational damage could be much worse. An executive said, *"It's something that has been described internally as the next payment protection insurance (PPI) if we don't get it right."*

## EU General Data Protection Regulation (GDPR)

The EU's General Data Protection Regulation (GDPR), which went into effect in May 2018, codifies and enshrines new consumer rights and organizational responsibilities. Financial institutions, like other businesses with customers and operations in the EU, have been scrambling to become GDPR-compliant. The regulation is focusing boardroom attention on compliance and readiness.

Among the GDPR's key provisions:

- It directs that contracts governing consent to use data be clear and easy to understand. Consumers must give unambiguous, affirmative, informed consent; data processors may no longer rely on 'opt in by default' or implied consent. Consumers also have the right to withdraw consent, a right that must be disclosed before consent is provided.
- It grants, or enshrines in law, new rights, including the right to know whether and how a firm is using an individual's data, rights to data access and portability, and the "right to be forgotten"—to have individual data erased and no longer disseminated.
- It imposes a 72-hour mandatory breach-notification requirement in cases where a breach is likely to "result in a risk for the rights and freedoms of individuals."[14]
- It requires organizations that process large amounts of sensitive personal data of EU residents to appoint a Data Protection Officer (DPO), who should report to the "highest management level," which could be the board of directors.[15]
- It imposes heavy maximum penalties for violations, as much as 4% of the firm's annual global revenue or €20 million, whichever is higher.[16]

Though GDPR only applies to firms that collect personal data on EU residents, some experts believe it may represent the leading edge of privacy regulation globally. A number of countries have already aligned their privacy laws with the GDPR, including Canada, Israel, and Japan; other countries are expected to follow suit.[17] Several participants said they expect similar regulations coming to the United States in some form. For example, in late June, California signed into law the California Consumer Privacy Act of 2018, which will give consumers the right to request all data businesses are collecting on them, as well as the right to request that businesses not sell any of their data.[18] The law, which goes into effect in 2020, also empowers the California attorney general to fine businesses for non-compliance.

*"We're seeing global banks thinking about whether they should just have one policy across the board globally."*

– EY Subject Matter Expert

As data privacy protection goes global, regulations are likely to continue taking different forms across jurisdictions, prompting some firms to consider an institutional response. An EY subject matter expert said, *"We're seeing global banks thinking about whether they should just have one policy across the board globally. Forward-thinking banks are considering getting ahead of this and doing it on an institutional level. Some are asking about GDPR-lite and how to implement that."* While firms continue to formulate the best global approach to GDPR, a participant noted it may be a long journey to compliance, *"Even in the EU, not a lot of banks are currently GDPR-compliant. It's a risk-based approach currently."*

## Access to bank data is expanding

While GDPR forces many businesses to more stringently protect data and to rethink how it is governed institutionally, other factors are pushing banks to open more of that data to third parties. The growth of fintech and data aggregation applications that rely on bank data is already expanding third-party access to financial institutions' core systems. Application programming interfaces (APIs) that enable third parties to access bank systems and data are providing new opportunities for banks to serve customers differently. Financial institutions can use APIs for reporting, giving clients better access to product processors, or offering additional services through third-party partnerships. Third-party applications typically layer on top of a provider's internal applications. Data aggregation apps, such as Mint or Personal Capital, are rising in popularity and help users track their spending habits by combining their various financial accounts into one snapshot. Bank account information is increasingly being shared with data aggregators so that customers can access third-party services.

Third-party access also brings a new set of risks for banks: competitive pressures and potential disintermediation from customers, as well as concerns about liability in the event of fraud.

## Regulations are forcing third-party access

*"How do you balance GDPR and open banking at the same time? One is asking you to be very careful with protecting data and how it is used, the other is forcing us to let third-parties in."*

– Participant

Regulations requiring banks to provide third-party access to data raise important questions about data ownership and accountability. The Payment Services Directive 2 (PSD2), aims to enhance consumer protection, promote innovation, and improve the security of payment services within the EU. One of PSD2's goals is encouraging competition, in part by requiring that financial institutions grant third parties access to some primary account-holder information. To address similar goals, the UK Competition and Markets Authority is implementing a program known as Open Banking, which enables customers to share data securely with other banks and third parties via APIs. UK banks will be required to allow consumers to share their own banking data with other banks and third parties, as well as manage multiple providers through a single app. The first stage of Open Banking aligned with PSD2 and became applicable in January 2018, though five of the nine biggest banks in the United Kingdom were granted extensions when they were unable to meet the deadline.

Open Banking is founded on the principle that data belongs to customers and not financial institutions—and that standards must be implemented to allow customers to take control of their data. Open Banking Implementation Trustee Imran Gulamhuseinwala noted that, while GDPR and PSD2 are *"technology agnostic, and didn't insist upon APIs,"* making Open Banking work requires *"data portability, which needs to be associated with data interoperability, and that requires a single standard among players."* He added, *"We provide enabling technology to customers, which allows them to execute financial transactions from third-parties on their behalf. We do that because the data is all very interesting and insightful, but unless it enables action at the end, it's not very valuable. And in financial services, doing something usually means transactions."*

Mr. Gulamhuseinwala also noted that Open Banking has the potential to enable everything from simple financial insights and product comparisons to "killer apps" in areas like customer onboarding, KYC, and identity verification. While it enables new ways for banks to do business, it also puts them in a difficult position. A participant asked, *"As a bank, how do you balance GDPR and open banking at the same time? One is asking you to be very careful with protecting data and how it is used, the other is forcing us to let third-parties in."*

The conflicting regulatory pressures muddy the waters for bank directors as they oversee broader business strategy. As one director put it, *"When we participate in PSD2 or Open Banking, how do we protect the data so that we do not violate GDPR? I wonder if the regulators behind each are even talking to each other or considering the implications."*

## Third-party relationships are raising questions about the value and uses of customer data

Though there are not yet similar open banking regulations outside of Europe, many large banks have already embraced the concept and are offering APIs to fintech firms and others, including data aggregators and accounting software providers.[19] All financial institutions must consider which third parties to partner with, how third parties should access and use bank data, and what the resultant risks or liabilities may be. Third-party relationships raise a number of important concerns for banks to consider, including:

- **Asymmetrical risks.** Large financial institutions are viewed differently from fintechs by both regulators and society at large. Given the unique space banks occupy, the tolerance for mistakes is far lower. *"It's easy for us to look at fintech players and their agility, but what we also need to do is remind ourselves of how little they have at risk when they make a mistake or have a failure,"* one director noted.
- **Concerns about liability.** Third party access to bank data, including accounts, could create new operational risks for banks. One participant pointed out: *"In a world of open banking, it appears risks are going up many times, and with that liability. Are we just taking on way more risk without any benefit?"* Others noted that banks may be held responsible for fraud or loss that occurs as a result of third-party access to customers' accounts, even if customers have authorized that access. One participant said, *"If systemic fraudulent action occurs and the bank has been forced by law to share their data with a third party, it's a rather unfortunate set of circumstances that mean a bank may have no fault whatsoever and yet may be held fully responsible."* A director highlighted that banks also often bear financial liability when third parties utilize bank product platforms and something goes wrong for the customer: *"When there is a problem, the bank absorbs the losses. That worries me as open banking expands. We need to be very vigilant about being the deep pockets of last resort. I think we'd all be shocked if we asked our corporate or consumer payments people about a breakdown of losses that should've likely been paid by others."* Another participant noted, *"We are talking about an ecosystem as*

*opposed to vertically integrated financial institutions. We need a legal liability framework underlying all of this."*

> *"This whole thing was always about competition. That typically involves a value shift in some sense."*
>
> – Imran Gulamhuseinwala

- **Competitive risks.** While global banks are positioned to compete in this environment given their vast customer base, capital, and relatively strong levels of customer trust, several participants asserted that the concept of open banking creates new competitive threats. Some participants shared the perspective that many of the presented benefits of the Open Banking regulation favor fintechs and tech companies—representing a potential industry value shift away from traditional players. Mr. Gulamhuseinwala suggested, however, that some banks could benefit: *"There are banks that get it, and they are using APIs, building marketplaces. The bank is becoming a third-party provider in some cases. This whole thing was always about competition. That typically involves a value shift in some sense."*

> *"I think this is going to be the real challenge moving forward. Do you become a utility bank? How do you not get disintermediated?"*
>
> – Director

- **Potential for disintermediation.** Perhaps the greatest concern is that banks will lose the direct interface with their customers and the data that comes with it, becoming back-end providers to more tech-savvy fintech firms for things like payments and financial management. A director said, *"I think this is going to be the real challenge moving forward. Do you become a utility bank? How do you not get disintermediated?"* To that end, some firms have initiated efforts to be a platform or aggregator themselves. HSBC recently became the first major UK bank to take advantage of Open Banking when it announced an app that centralizes customer account information across accounts, even those that are held with rival firms. Both customers and non-customers will be able to integrate their financial information into the app and access other financial tools and providers.[20] Some firms are building collections of company-owned fintechs to maintain control of the customer relationship. Smart money application Yolt, a fintech subsidiary of ING, was the first third-party provider to complete a successful connection under the Open Banking system.[21]

## Data opportunities and risks require a strategic approach to data management and governance

The myriad opportunities data presents to better serve customers offer great potential, but they also pose clear strategic challenges, ethical questions, and operational obstacles that likely must be overcome first. Bank leaders are faced with a difficult balancing act: investing in the ability to better manage and use data, while ensuring compliance with new regulations, addressing changing customer perceptions about privacy, and minimizing the potential loss of control of data. One participant's board is asking if there may be an advantage to having less data rather than more. The participant explained: *"The board needs to understand the data it believes it needs to hold for the purpose of the business. You may actually conclude that you want to hold as little as possible."* Bank boards must be involved in overseeing the direction their firms take in tackling these obstacles. Given the potential value to be unlocked and the risks, banks need a strategic approach to data.

## Boards are beginning to raise questions around data strategy

*"We're not having enough of a strategic discussion about data yet … Most banks are still grappling with figuring out what data they currently have and how to use it."*

– Director

Historically, many financial institutions approached data governance as a compliance exercise or focused specifically on security. A privacy expert shared with Tapestry why it is so vital for boards and management to think beyond compliance: *"On one hand, data conversations have become very compliance-driven due to new regulations, but at the same time their organizations have become very aggressive with data. They need to be thinking outside the box to ensure that the use of data is appropriate. This is a very real risk for these companies."* The scale of the investment needed to get the IT architecture right and the strategic importance of data is beginning to broaden the scope of data conversations and making an institution's approach to data a key aspect of business strategy. Banking leaders are beginning to have some fundamental discussions about data. *"This is a topic that is certainly being elevated as a priority in our boardroom,"* one director said. Another participant agreed, noting, *"It's now moving beyond just a risk discussion and is about risks in relation to the data strategy. That strategy encompasses technology, data, and opportunities—and the risks associated with it."*

For many boards, particularly for those with large retail consumer businesses in Europe, efforts thus far have focused largely around managing shifting regulatory requirements—such as GDPR and Open Banking—and privacy concerns around personal data. Further, many banks are still getting up to speed in figuring out what their data assets are and what the technical obstacles are to employ that data effectively. One director said, *"We're not having enough of a strategic discussion about data yet. I think most banks are still grappling with figuring out what data they currently have and how to use it."*

Diverse, global banks are likely too complex for leaders to establish a single encompassing "data strategy" across the organization. A participant said, *"I think the point here is that there is not just one data strategy. I think we tend to try to simplify it. A lot of this is just about ensuring that we think about these implications across different businesses and the different uses of data."*

### Establishing core principles around data use

To protect their reputations and maintain trust, banks need to develop some core principles about how they will use data and be prepared to explain their data practices to customers. Most banks are still at the beginning of these discussions. A director said, *"I think we're early days in this area as financial institutions. Having that sufficient maturity within our organizations where we're clear on those rules—that's a journey."* An executive suggested boards should start by asking some fundamental questions of management: *"There's a basic infrastructure that a board should be asking management about: How is data flowing within the company? How are you sourcing data and who are you sharing it with? How accurate is that data and how is it being used? Can they show you that and verify it?"*

> *"We will very quickly get to the point where we can conduct very advanced data analytics. We will have to ask ourselves, just because we can, should we?"*
>
> – Executive

Boards and management need to establish data strategies that consider not only what their firms can do with data, but also what they should and will do based on shifting societal and ethical norms and customer expectations. An executive said, *"Each institution should have a set of legally produced guidelines around data. It's painstaking and onerous, but it's a process you simply have to go through, because if you get it wrong, the risks are incredibly high."*

Participants identified a few key areas where data usage may pose ethical questions and/or present reputational risks:

- **Customer profiling.** An executive said, *"We will very quickly get to the point where we can conduct very advanced data analytics. We will have to ask ourselves, just because we can, should we? You can wind up looking at people and profiling based on where they live, age, race, etc. What does that say about our institution and industry? It will be legal, but will it be ethical?"*
- **Offering advice or "nudging" customers.** Firms want to use data to create a more tailored banking environment that better serves customers, but those efforts raise questions about what level of personalization customers will be comfortable with. An executive explained, *"There are challenges when it comes to taking the data we have and using it for nudging. If a customer is in a car showroom and suddenly they get an offer for car financing, is that creepy or reasonable? If you're Google it's reasonable, if you're a bank it's probably a little creepy."* A director asked what the expectation is for banks to assist customers as data and technology expand the ability to do so: *"If you see someone is using the wrong account or not handling their debt properly, what is our role? We have the*

*data now that could really guide customers, but are we going to play mother to them? Is that even something they want?"*

- **Automating the decision process.** A director said, *"When I reflect on our prior conversations around artificial intelligence and automation—the value of that stuff is made possible by data, and that has implications that we probably do not yet fully understand."* Many in the industry believe automated systems create new risks related to concerns about fake data, external data manipulation, and inherent bias.[22] One participant said, *"The use and abuse of big data is a major concern for me. Algorithms are very good at correlations, but not so good at dealing with cause and effect and treating customers fairly."* A regulator agreed, noting, *"You really need to test the outcomes, because you can easily build biases in without malicious intent. You need to look at the outcomes to ensure they are reasonable. Now, the board wouldn't do that, but they should be directing others to do so."* A recent survey found three out of four banks are not well-prepared to face the societal and liability issues that come with having algorithms making customer-facing decisions on a daily basis.[23] Another participant stated, *"These are tools. We cannot rely on them as the sole arbiters. Classic risk management techniques won't apply."*

*"You are taking a great risk if you can't assure the quality and provenance of the data you are using."*

– Director

- **Ensuring data quality.** Several participants expressed concerns about the integrity of the data their firms maintain and utilize. A director said, *"The quality of data is vital. You are taking a great risk if you can't assure the quality and provenance of the data you are using."* Research suggests banks may be particularly vulnerable to bad data. A recent survey found that, while 84% of bankers agree that their firms are increasingly using data to drive critical decision making, 77% believe most banks are not prepared to confront corrupted insights, bad decisions, and potential compliance failures that may result from falsified data entering their systems.[24]

## Updating systems to enable effective use of data

As part of their digital transformation efforts, many firms are in the midst of slowly updating antiquated systems that have been pieced together over time. A participant said in a pre-meeting conversation, *"We know what the right IT architecture is. If you are building your platform from scratch and thinking about design, the principles are well known. You can get it 95% right. The challenge is that almost no one is building their platforms from scratch; they're trying to retrofit it onto a legacy platform, and that's tough."* As firms work to improve their systems, there is a range of potentially conflicting objectives. For bank data to be utilized to its full potential, it needs to be better consolidated and easier to manage, but it also must be sufficiently protected throughout the process. A recent attempt by TSB Bank, a retail and commercial bank in the United Kingdom, to migrate its systems after being acquired illustrates the challenges and risks of major system upgrades. TSB's IT migration efforts resulted in a very public meltdown that has affected 1.3 billion customer records and 1.9 million of the bank's 5.4 million customers.[25]

> *"Everything about our systems has been designed to not be able to delete or lose data."*
>
> – Executive

As previously noted, GDPR enshrines an EU citizen's "right to be forgotten"—to have individual data erased and no longer disseminated. An executive explained why this is particularly difficult in financial services versus other industries: *"Data deletion? Everything about our systems has been designed to not be able to delete or lose data."* A director agreed, saying, *"If somebody says, 'forget me,' I'd love to tell you our backend service lines and legacy systems are up to speed and know where every person's data exists across the board, but that's just not the case. It's very difficult. I believe this whole idea of being forgotten could be the next big fine area for banks."*

## Banks are considering the appropriate management structure

In January 2013, the Basel Committee on Banking Supervision released standard number 239 (BCBS 239) in an effort to strengthen banks' risk data aggregation capabilities and internal risk reporting practices. Driven by the global financial crisis, BCBS 239 qualified regulators' expectations of banks regarding formal roles and responsibilities for data.[26] In response, many firms created a chief data officer (CDO) role where one did not previously exist or assigned various data governance responsibilities to existing roles. This has resulted in questions and inconsistencies about who holds ultimate responsibility with respect to data oversight, as well as who reports to the board on these issues.

> *"If you're going out and hiring a new CDO but still hiring the same people elsewhere, I think you're missing the point … We all need to be data executives now."*
>
> – Executive

Some participants asked whether the broader strategic importance of data and the balancing of priorities needed to get data management right suggest the need for the CDO role to be elevated to the C-suite. Most participants did not support a centralized, senior owner of data strategy. An executive stated, *"I quite passionately believe we need to better handle how we think of this. If you're going out and hiring a new CDO but still hiring the same people elsewhere, I think you're missing the point. The people on the executive side need to have a depth of understanding about data and technology that was never required before. We all need to be data executives now."* Most participants agreed that it's the business lines that need to own the data agenda—not IT or an elevated CDO role. Several participants emphasized the need for business lines to own responsibility for their data strategy: *"Our view is that the businesses and functions own the data, and the CDO function is to ensure the quality of that data. We have distributed CDOs across business lines and maintaining data quality at certain levels is tied to compensation."* One regulator said the title is not important, as long as data is being used appropriately to ensure the safety and soundness of the institution and industry.

★★★

Banks face a future where their institutional approach to data will be a critical part of their success or failure. Not all regulatory regimes have the teeth of the GDPR or the business model implications of Open Banking, but regulations and consumer expectations are moving toward a greater emphasis on privacy and consumer control of their data. Failure to comply with regulations or a major data breach could bring significant fines and, more importantly, significant reputational damage. Growing competitive pressures and changes in customer behavior represent real threats for the industry—but in some ways financial institutions are well-positioned to face those challenges if they can effectively tap into the resources at their disposal. Winning business models will require the institution's ability to gather and analyze data on a massive scale, and whether and how well firms will be able to do so remains an open question with significant challenges ahead. Boards are at the beginning of a long-term discussion about how to make the most of their data.

## *About this document*

### About *ViewPoints*

*ViewPoints* reflects the network's use of a modified version of the Chatham House Rule whereby names of network participants and their corporate or institutional affiliations are a matter of public record, but comments are not attributed to individuals, corporations, or institutions. Network participants' comments appear in italics.

### About the Bank Governance Leadership Network (BGLN)

The BGLN addresses key issues facing complex global banks. Its primary focus is the non-executive director, but it also engages members of senior management, regulators, and other key stakeholders committed to outstanding governance and supervision in support of building strong, enduring, and trustworthy banking institutions. The BGLN is organized and led by Tapestry Networks, with the support of EY. *ViewPoints* is produced by Tapestry Networks and aims to capture the essence of the BGLN discussion and associated research. Those who receive *ViewPoints* are encouraged to share it with others in their own networks. The more board members, senior management, advisers, and stakeholders who become engaged in this leading edge dialogue, the more value will be created for all.

### About Tapestry Networks

Tapestry Networks is a privately held professional services firm. Its mission is to advance society's ability to govern and lead across the borders of sector, geography, and constituency. To do this, Tapestry forms multi-stakeholder collaborations that embrace the public and private sector, as well as civil society. The participants in these initiatives are leaders drawn from key stakeholder organizations who realize the status quo is neither desirable nor sustainable, and are seeking a goal that transcends their own interests and benefits everyone. Tapestry has used this approach to address critical and complex challenges in corporate governance, financial services, and healthcare.

### About EY

EY is a global leader in assurance, tax, transaction, and advisory services to the banking industry. The insights and quality services it delivers help build trust and confidence in the capital markets and in economies the world over. EY develops outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, EY plays a critical role in building a better working world for its people, for its clients, and for its communities. EY supports the BGLN as part of its continuing commitment to board effectiveness and good governance in the financial services sector.

## Appendix: discussion participants

In June of this year, Tapestry and EY hosted two BGLN meetings on the emerging opportunities and risks of data in banking. These meetings included more than 35 conversations with directors, executives, regulators, supervisors, and other thought leaders. Insights from these discussions informed this *ViewPoints*, and unattributed quotes from these discussions appear throughout.

The following individuals participated in BGLN discussions on the emerging opportunities and risks of data in banking:

### BGLN Participants

- Hilary Ackerman, Risk Committee Chair, Credit Suisse USA
- Homaira Akbari, Non-Executive Director, Santander
- Mike Ashley, Audit Committee Chair, Barclays
- Colin Bell, Group Head, Financial Crime Risk, HSBC
- Ann Borowiec, Non-Executive Director, Santander Bank NA and Audit Committee Chair, Banco Santander International
- Nida Davis, Associate Director, Division of Supervision and Regulation, Federal Reserve System
- David Denison, Audit Committee Chair, RBC
- JP Donleavy, Executive Manager, Data Operations, BNY Mellon
- Beth Dugan, Deputy Comptroller, Operational Risk, Office of the Comptroller of the Currency
- Terri Duhon, Risk Committee Chair, Morgan Stanley International
- Imran Gulamhuseinwala, Implementation Trustee, Open Banking Initiative, and Global Head of FinTech, EY
- Bob Herz, Audit Committee Chair, Morgan Stanley
- Christine Hodgson, Senior Independent Director and Remuneration Committee Chair, Standard Chartered
- Phil Kenworthy, Non-Executive Director, ClearBank
- Bridget van Kralingen, Non-Executive Director, RBC
- Richard Meddings, Audit Committee Chair, Deutsche Bank
- Debby McWhinney, Non-Executive Director, Lloyds Banking Group
- Clair Mills, Head, Change & Data Management, UK Prudential Regulation Authority
- Tom Noyes, Founder & CEO, Commerce Signals
- Naoyuki Oguri, Senior Managing Director, Data Management Officer, and Global Head, Data Management Office, Nomura

- Andy Ozment, Chief Information Security Officer, Goldman Sachs
- Kevin Parry, Audit Committee Chair, Nationwide Building Society
- Jane Peverett, Audit Committee Chair, CIBC
- Jim Quigley, Audit & Examination Committee Chair, Wells Fargo
- Thomas Renyi, Non-Executive Director, RBC
- Michael Schoch, Head, Banks Division, FINMA
- David Sidwell, Senior Independent Director and Risk Committee Chair, UBS
- John Sutherland, Senior Advisor, UK Financial Conduct Authority
- John Tattersall, Chair of the Board, UBS Limited
- Michele Trogni, Non-Executive Director, Deutsche Bank
- Suzanne Vautrinot, Non-Executive Director, Wells Fargo
- Todd Vermilyea, Senior Associate Director, Division of Supervision and Regulation, Federal Reserve System
- Tom Woods, Non-Executive Director, Bank of America

## EY

- Omar Ali, Managing Partner, UK Financial Services
- Andy Baldwin, Area Managing Partner, EMEIA
- Angus Champion de Crespigny, Cryptoasset Leader, Financial Services
- John Doherty, Partner, Information Technology Advisory Practice
- Scott Keipper, Principal, Advisory, Financial Services
- Isabelle Santenac, Assurance Managing Partner, EMEIA
- Bill Schlich, Global Banking & Capital Markets Leader
- Hamish Thomas, Partner, EMEIA Financial Services Office Advisory and UK Head, Banking Technology

## Tapestry Networks

- Dennis Andrade, Partner
- Brennan Kerrigan, Associate
- Tucker Nielsen, Principal

# Endnotes

[1] Kian Bakhtiari, "The Dangers of Data: Why the Numbers Never Tell the Full Story," World Economic Forum, April 18, 2018.

[2] Amit Garg, David Grande, Gloria Macias-Lizaso Miranda, Christoph Sporieder, and Eckart Windhagen, "Analytics in Banking: Time to Realize the Value," McKinsey & Company, April 2017.

[3] Kai Keller, "Data Protection Standards Need to be Global," *Wired*, April 29, 2018.

[4] John Koetsier, "Digital Duopoly Declining? Facebook's, Google's Share of Digital Ad Dollars Dropping," *Forbes*, March 19, 2018.

[5] Prasad Chintamaneni, "How Banks are Capitalizing on a New Wave of Bog Data and Analytics," (Sponsor Content from Cognizant) *Harvard Business Review*, November 22, 2016.

[6] Jim Marous, "Citibank Launches PFM Mobile App to Steal Customers," *The Financial Brand*, accessed May 16, 2018.

[7] Sooraj Shah, "NatWest Prevented £7m of Corporate Fraud Using Machine Learning," *Internet of Business*, April 6, 2018.

[8] Sarah Ponczek, "Machines Poised to Take Over 30% of Work at Banks, McKinsey Says," *Bloomberg,* July 20, 2017.

[9] Bruce Sterling, "Tech-Lash Galore," *Wired*, April 30 2018.

[10] "ABA Survey: Six in Ten Consumers Trust Banks Most to Safeguard Payments," *ABA Banking Journal*, October 9, 2017.

[11] Mary Wisniewski, "Facebook's Data Problems Have an Upside for Banks," *American Banker*, April 10, 2018.

[12] Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," *The New York Times*, April 4, 2018.

[13] "GDPR Key Changes," EU GDPR Portal. For more information on the GDPR, see EY, *GDPR: Demanding New Privacy Rights and Obligations—Perspectives for Non-EU Financial Services Firms* (London: EYGM Limited, 2017).

[14] "GDPR Key Changes," GDPR Portal, accessed December 14, 2017.

[15] EY, *GDPR: Demanding New Privacy Rights and Obligations Perspectives for Non-EU Financial Services Firms* (London: EYGM Limited, 2017).

[16] "GDPR Key Changes," EU GDPR Portal. For more information on the GDPR, see EY, *GDPR: Demanding New Privacy Rights and Obligations Perspectives for Non-EU Financial Services Firms* (London: EYGM Limited, 2017).

[17] Nuala O'Connor, "Reforming the US Approach to Data Protection and Privacy," Council on Foreign Relations, January 30, 2018.

[18] Janko Roettgers, "California's New Privacy Law Could Have Big Impact on Tech, Media," *Variety*, June 29, 2018.

[19] Penny Crosman, "Why Do Most US Banks Shut the Door on 'Open Banking?'" *American Banker*, December 20, 2017.

[20] Hannah Durevall, "HSBC Embraces Open Banking and Aggregation Platforms," *Mapa Research*, October 29, 2017.

[21] Douglas Blakey, "ING's Fintech Subsidiary Yolt Scores UK Open Banking First With Lloyds," *Retail Banker International*, January 25, 2018.

[22] Alan McIntyre, Kelley Conway, Peter Sidebottom, Schira Lillis, and Peter McElwaine-Johnn, *Building the Future-Ready Bank: Banking Technology Vision 2018* (Accenture, 2018), 16.

[23] McIntyre, Conway, Sidebottom, Lillis, and McElwaine-Johnn, *Building the Future-Ready Bank: Banking Technology Vision 2018*, 6.

[24] McIntyre, Conway, Sidebottom, Lillis, and McElwaine-Johnn, *Building the Future-Ready Bank: Banking Technology Vision 2018*, 16.

[25] Chris Stokel-Walker, "We're On Our Knees': Inside the Totally Avoidable TSB Crisis," *Wired*, May 1, 2018.

[26] Guy Pearce, "Align Data Governance with Board Governance Imperatives," *The Data Administration Newsletter*, May 3, 2017.