Contributions for assisting in the future recovery and resolution of the Spanish banking sector may have a material adverse effect on the Bank's business, financial condition and results of operations

Spanish credit institutions, including BBVA, are required to make at least one annual ordinary contribution to the National Resolution Fund (*Fondo de Resolución Nacional*) ("**FRN**"), payable on request of the FROB. The total amount of contributions by all Spanish banking entities must equal at least 1% of the aggregate amount of all deposits guaranteed by the Credit Entities Deposit Guarantee Fund (*Fondo de Garantía de Depósitos de Entidades de Crédito*) ("**FGD**") by December 31, 2024. The contributions are adjusted to the risk profile of each institution in accordance with the criteria set out in the relevant regulation. Moreover, the FROB may decide to collect additional contributions. Furthermore, Law 11/2015 establishes an additional contribution that seeks to provide financing to the FROB in its capacity as the Spanish Resolution Authority. This contribution amounts to 2.5% of the aforementioned annual ordinary contribution to the FRN. Finally, since 2016, the Bank is required to make contributions directly to the Single Resolution Fund.

Any funding requirements imposed on the Bank pursuant to the foregoing or otherwise in any of the jurisdictions in which it operates could have a material adverse effect on the Bank's business, financial condition and results of operations.

Our financial results, regulatory capital and ratios may be negatively affected by changes to accounting standards

We report our results and financial position in compliance with IFRS-IASB and in accordance with EU-IFRS required to be applied under the Bank of Spain's Circular 4/2017, which replaced the Bank of Spain's Circular 4/2004 for financial statements relating to periods ended January 1, 2018 and thereafter. Changes to IFRS or interpretations thereof may cause our future reported results and financial position to differ from current expectations or historical results, or historical results to differ from those previously reported due to the adoption of accounting standards on a retrospective basis. Such changes may also affect our regulatory capital and ratios. We monitor potential accounting changes and, when possible, we determine their potential impact and disclose significant future changes in our financial statements that we expect as a result of those changes. Currently, there are a number of issued but not yet effective IFRS changes, as well as potential IFRS changes, some of which could be expected to impact our reported results, financial position and regulatory capital in the future. For further information about developments in financial accounting and reporting standards, see Note 2.3 to our Consolidated Financial Statements ("Recent IFRS pronouncements").

Tax Risks

Increased taxation and other burdens may have a material adverse effect on the Bank's business, financial condition and results of operations

On February 14, 2013, the European Commission published a proposal (the "**Commission's Proposal**") for a directive for a common financial transaction tax (the "**EU FTT**") in Belgium, Germany, Estonia, Greece, Spain, France, Italy, Austria, Portugal, Slovenia and Slovakia (the "**participating Member States**"). However, Estonia has since stated that it will not participate.

The Commission's Proposal has very broad scope and could, if implemented, apply to certain dealings in securities issued by the Group or other issuers (including secondary market transactions) in certain circumstances.

Under the Commission's Proposal, the EU FTT could apply in certain circumstances to persons both within and outside the participating Member States. Generally, it would apply to certain dealings in securities where at least one party is a financial institution and at least one party is established in a participating Member State. A financial institution would be considered to be "established" in a participating Member State in a broad variety of circumstances, including: (i) by carrying out transactions with a person established in a participating Member State or (ii) when the financial instrument involved in the transaction has been issued in a participating Member State.

However, the Commission's Proposal remains subject to negotiation among the participating Member States. It may therefore be altered prior to any implementation, the timing of which remains unclear. Additional EU Member States may decide to participate, and participating Member States may decide not to participate.

While the final outcome of the Commission's Proposal continues to be uncertain, in February 2020 a financial transaction tax was announced in Spain which is based in part on the Commission's Proposal (the "**Spanish FTT**"). The Spanish FTT rate is proposed to be 0.2%, to be charged on acquisitions of shares in Spanish companies, regardless of the tax residence of the participants in such transactions, provided that such companies are listed and their respective market capitalization is above €1,000 million. Trades of the Bank's shares would be subject to the Spanish FTT. If the directive for the implementation of the EU FTT is approved, the Spanish FTT would have to be adapted to the content of the directive. The EU FTT could impose a higher tax rate than that currently proposed in the Spanish FTT bill.

There can be no assurance that additional financial transaction taxes will not be adopted by the authorities of the jurisdictions where the Bank operates and, if introduced, certain financial instrument transactions may be subject to higher expenses.

Any levies or taxes imposed on the Bank's securities or activities or otherwise affecting the Bank pursuant to the foregoing or otherwise could have a material adverse effect on the Bank's business, financial condition and results of operations.

Reporting Risks

BBVA's financial statements are based in part on assumptions and estimates which, if inaccurate, could cause material misstatement of the results of its operations and financial position

The preparation of financial statements in compliance with IFRS-IASB requires the use of estimates. It also requires management to exercise judgment in applying relevant accounting policies. The key areas involving a higher degree of judgment or complexity, or areas where assumptions are significant to the consolidated and individual financial statements, include the classification, measurement and impairment of financial assets, particularly where such assets do not have a readily available market price, the assumptions used to quantify certain provisions and for the actuarial calculation of post-employment benefit liabilities and commitments, the useful life and impairment losses of tangible and intangible assets, the valuation of goodwill and purchase price allocation of business combinations, the fair value of certain unlisted financial assets and liabilities, the recoverability of deferred tax assets and the exchange and inflation rates of Venezuela. There is a risk that if the judgment exercised or the estimates or assumptions used subsequently turn out to be incorrect then this could result in significant loss to the Group beyond that anticipated or provided for, which could have an adverse effect on the Group's business, financial condition and results of operations.

Observable market prices are not available for many of the financial assets and liabilities that the Group holds at fair value and a variety of techniques to estimate the fair value are used. Should the valuation of such financial assets or liabilities become observable, for example as a result of sales or trading in comparable assets or liabilities by third parties, this could result in a materially different valuation to the current carrying value in the Group's financial statements.

The further development of standards and interpretations under IFRS-IASB could also significantly affect the results of operations, financial condition and prospects of the Group. See "*—Legal Risks—Regulatory Risks—Our financial results, regulatory capital and ratios may be negatively affected by changes to accounting standards*".

INTERNAL CONTROL RISKS

Compliance Risks

The Group is exposed to compliance risks which may have a material adverse effect on the Group's business, financial condition and results of operations, and may damage the Group's reputation

As part of its business, the Group offers and markets banking and investment products and services to its customers and actively operates in financial markets on its own behalf and on behalf of its customers in the various jurisdictions in which it operates. As a result of the nature of its operations and the fact that the Group operates in many different jurisdictions around the world, the Group must comply with a wide array of laws, rules and regulations, many of which have different scopes and implications. Legal fragmentation may be further exacerbated by how such laws, rules and regulations are implemented by the relevant local supervising authorities. This fragmentation makes compliance risk management particularly complex, as compliance programs must address the different legal requirements facing the Group.

Compliance risk relates to the fact that the Group must comply with many different laws, rules and regulations. For example, the Group is subject to laws, rules and regulations regarding money laundering and the financing of terrorism. The Group must also abide by applicable sanctions programs. The most relevant sanctions programs are those administered by the United Nations, the European Union and the United States (including sanctions imposed by the Office of Foreign Assets Control under the U.S. Treasury Department). In addition, the Group's operations are subject to various anti-corruption laws, including the U.S. Foreign Corrupt Practices Act of 1977 and the UK Bribery Act of 2010. These anti-corruption laws generally prohibit providing anything of value to government officials for the purposes of obtaining or retaining business or securing any improper business advantage. As part of the Group's business, the Group may directly or indirectly, through third parties, deal with entities whose employees are considered to be government officials. The Group's activities are also subject to complex customer protection and market integrity regulations.

The Group has compliance programs intended to mitigate the Group's compliance risk. However, the Group cannot provide assurance that the controls established within the Group to ensure compliance with these laws, rules and regulations will not be circumvented or that they will otherwise be sufficient to prevent their violation. A violation of the applicable laws, rules and regulations could lead to material consequences, including financial penalties being imposed on the Group, limits being placed on the Group's activities, the Group's authorizations and licenses being revoked, damage to the Group's reputation and other consequences, any of which could have a material adverse effect on the Group's business, results of operations and financial condition.

Further, compliance with these laws, rules and regulations can represent a material financial burden for the Group and raise important technical problems. Further, the Group engages in investigations relating to potential violations of these laws, rules and regulations from time to time and any such investigations or any related proceedings could be time-consuming and costly and their outcomes difficult to predict.

Moreover, some of our management, employees and/or persons doing business with us may engage in activities that are incompatible with our ethics and compliance standards. Although we have adopted measures designed to identify, monitor and mitigate such actions, and remediate them when we become aware of them, we are subject to the risk that such persons may engage in fraudulent activity, corruption or bribery, circumvent or override our internal controls and procedures or misappropriate or manipulate our assets for their personal or business advantage to our detriment.

Our business, including relationships with third parties, is guided by ethical principles. We have adopted a Code of Conduct, applicable to all companies and persons which form part of the Group, and a number of internal policies designed to guide our management and employees and reinforce our values and rules for ethical behavior and professional conduct. However, we are unable to ensure that all of our management and employees, more than 125,000 people, or persons doing business with us comply at all times with our ethical principles. Acts of misconduct by any employee, and particularly by senior management, could erode trust and confidence and damage the Group's reputation among existing and potential clients and other stakeholders. Actual or alleged misconduct by Group entities in any number of activities or circumstances, including operations, employment-related offenses such as sexual harassment and discrimination, regulatory compliance, the use and protection of data and systems, and the satisfaction of client expectations, and actions taken by regulators or others in response to such misconduct, could lead to, among other things, sanctions, fines and reputational damage, any of which could have a material adverse effect on the Group's business, financial condition and results of operations.

IT Risks

Weaknesses or failures in the Group's internal or outsourced processes, systems and security could materially adversely affect its business, financial condition and results of operations and could result in reputational damage

Operational risks, through inadequate or failed internal processes, systems (including financial reporting and risk monitoring processes) or security, or from people-related or external events, including the risk of fraud and other criminal acts carried out by Group employees or against Group companies, are present in the Group's businesses. These businesses are dependent on processing and reporting accurately and efficiently a high volume of complex transactions across numerous and diverse products and services, in different currencies and subject to a number of different legal and regulatory regimes. Any weakness in these internal processes, systems or security could have an adverse effect on the Group's results, the reporting of such results, and on the ability to deliver appropriate customer outcomes during the affected period. In addition, any breach in security of the Group's systems could disrupt its business, result in the disclosure of confidential information and create significant financial and legal exposure for the Group. Although the Group devotes significant resources to maintain and regularly update its processes and systems that are designed to protect the security of its systems, software, networks and other technology assets, there is no assurance that all of its security measures will provide absolute security. Furthermore, the Group has outsourced certain functions (such as the storage of certain information) to third parties and, as a result, it is dependent on the adequacy of the internal processes, systems and security measures of such third parties. Any actual or perceived inadequacies, weaknesses or failures in the Group's systems, processes or security or the systems, processes or security of such third parties could damage the Group's reputation (including harming customer confidence) or could otherwise have a material adverse effect on its business, financial condition and results of operations.

The Group faces security risks, including denial of service attacks, hacking, social engineering attacks targeting its partners and customers, malware intrusion or data corruption attempts, and identity theft that could result in the disclosure of confidential information, adversely affect its business or reputation, and create significant legal and financial exposure.

The Group's computer systems and network infrastructure and those of third parties, on which it is highly dependent, are subject to security risks and could be susceptible to cyber-attacks, such as denial of service attacks, hacking, terrorist activities or identity theft. The Group's business relies on the secure processing, transmission, storage and retrieval of confidential, proprietary and other information in its computer and data management systems and networks, and in the computer and data management systems and networks of third parties. In addition, to access the Group's network, products and services, its customers and other third parties may use personal mobile devices or computing devices that are outside of its network environment and are subject to their own cybersecurity risks.

The Group, its customers, regulators and other third parties, including other financial services institutions and companies engaged in data processing, have been subject to, and are likely to continue to be the target of, cyber-attacks. These cyber-attacks include computer viruses, malicious or destructive code, phishing attacks, denial of service or information, ransomware, improper access by employees or vendors, attacks on personal email of employees, ransom demands to not expose security vulnerabilities in the Group's systems or the systems of third parties or other security breaches that could result in the unauthorized release, gathering, monitoring, misuse, loss or destruction of confidential, proprietary and other information of the Group, its employees, its customers or of third parties, damage its systems or otherwise materially disrupt the Group's or its customers' or other third parties' network access or business operations. As cyber threats continue to evolve, the Group may be required to expend significant additional resources to continue to modify or enhance its protective measures or to investigate and remediate any information security vulnerabilities or incidents. Despite efforts to ensure the integrity of the Group's systems and implement controls, processes, policies and other protective measures, the Group may not be able to anticipate all security breaches, nor may it be able to implement guaranteed preventive measures against such security breaches and the measures implemented by the Group may not be sufficient. Cyber threats are rapidly evolving and the Group may not be able to anticipate or prevent all such attacks and could be held liable for any security breach or loss.

Cybersecurity risks for banking organizations have significantly increased in recent years in part because of the proliferation of new technologies, and the use of the internet and telecommunications technologies to conduct financial transactions. For example, cybersecurity risks may increase in the future as the Group continues to increase its mobile-payment and other internet-based product offerings and expand its internal usage of web-based products and applications. In addition, cybersecurity risks have significantly increased in recent years in part due to the increased sophistication and activities of organized criminal groups, terrorist organizations, hostile foreign governments, disgruntled employees or vendors, activists and other external parties, including those involved in corporate espionage. Even the most advanced internal control environment may be vulnerable to compromise. Targeted social engineering attacks and “spear phishing” attacks are becoming more sophisticated and are extremely difficult to prevent. In such an attack, an attacker will attempt to fraudulently induce colleagues, customers or other users of the Group’s systems to disclose sensitive information in order to gain access to its data or that of its clients. Persistent attackers may succeed in penetrating the Group’s defenses given enough resources, time, and motive. The techniques used by cyber criminals change frequently, may not be recognized until launched and may not be recognized until well after a breach has occurred. The risk of a security breach caused by a cyber-attack at a vendor or by unauthorized vendor access has also increased in recent years. Additionally, the existence of cyber-attacks or security breaches at third-party vendors with access to the Group’s data may not be disclosed to it in a timely manner.

The Group also faces indirect technology, cybersecurity and operational risks relating to the customers, clients and other third parties with whom it does business or upon whom it relies to facilitate or enable its business activities, including, for example, financial counterparties, regulators and providers of critical infrastructure such as internet access and electrical power. As a result of increasing consolidation, interdependence and complexity of financial entities and technology systems, a technology failure, cyber-attack or other information or security breach that significantly degrades, deletes or compromises the systems or data of one or more financial entities could have a material impact on counterparties or other market participants, including the Group. This consolidation, interconnectivity and complexity increase the risk of operational failure, on both individual and industry-wide bases, as disparate systems need to be integrated, often on an accelerated basis. Any third-party technology failure, cyber-attack or other information or security breach, termination or constraint could, among other things, adversely affect the Group’s ability to effect transactions, service its clients, manage its exposure to risk or expand its business.

Cyber-attacks or other information or security breaches, whether directed at the Group or third parties, may result in a material loss or have material consequences. Furthermore, the public perception that a cyber-attack on its systems has been successful, whether or not this perception is correct, may damage the Group’s reputation with customers and third parties with whom it does business. Hacking of personal information and identity theft risks, in particular, could cause serious reputational harm. A successful penetration or circumvention of system security could cause the Group serious negative consequences, including loss of customers and business opportunities, significant business disruption to its operations and business, misappropriation or destruction of its confidential information and/or that of its customers, or damage to the Group’s or its customers’ and/or third parties’ computers or systems, and could result in a violation of applicable privacy laws and other laws, litigation exposure, regulatory fines, penalties or intervention, loss of confidence in the Group’s security measures, reputational damage, reimbursement or other compensatory costs, additional compliance costs, and could adversely impact its results of operations, liquidity and financial condition.

The financial industry is increasingly dependent on information technology systems, which may fail, may not be adequate for required tasks or may no longer be available

Our activities are increasingly dependent on highly sophisticated information technology (“**IT**”) systems. IT systems are vulnerable to a number of problems, such as software or hardware malfunctions, computer viruses, hacking and physical damage to vital IT centers. IT systems need regular upgrading and the Bank may not be able to implement necessary upgrades on a timely basis or upgrades may fail to function as planned.

Furthermore, the Group is under continuous threat of loss due to cyber-attacks, especially as it continues to expand customer capabilities to utilize internet and other remote channels to transact business. Two of the most significant cyber-attack risks that it faces are e-fraud and breach of sensitive customer data. Loss from e-fraud occurs when cybercriminals breach and extract funds directly from customers’ or the Group’s accounts. A breach of sensitive customer data, such as account numbers, could present significant reputational impact and significant legal and/or regulatory costs to the Group.