Code of Business Conduct 2018

TABLE OF CONTENTS

Page

ARCH CAPITAL GROUP LTD.
Code of Business Conduct

GENERAL STATEMENT

Arch Capital Group Ltd. ("ACGL") and its controlled subsidiaries (together with ACGL, the "Company") are committed to integrity in the conduct of their business and require that all Employees (as defined below) perform their duties in a manner which is legally, ethically and morally irreproachable. Our Board of Directors and senior management have made the development of an organizational culture that encourages compliance with the highest ethical standards one of our first priorities. The Company's standards are clear: simply complying with laws or following widespread business practices may be insufficient.

To implement ACGL's commitment to integrity in the conduct of our business, we have adopted a Code of Business Conduct (the "Code") and a series of policy statements (the "Policy Statements"), as well as a Compliance and Ethics Program which is designed to ensure that we have in place policies and systems designed to prevent and detect violations of our Code and Policy Statements and to be able to respond appropriately to any violations and to prevent further violations.

The Code and Policy Statements describe the ethical principles the Company has set for the conduct of its business, and outline certain key legal requirements of which all Employees should be generally aware. Compliance with these requirements, together with any additional requirements applicable to any subsidiary, branch or other local operation of the Company under applicable local laws, is mandatory. While adherence to the principles set forth herein is a condition of employment at the Company, no employment contract is intended or offered by reason of this Code. Violations will not be tolerated and may result in one or more of the following: warnings, reprimands, probation, demotion, temporary suspension, reimbursement of the Company's losses or damages, discharge or any other actions as may be appropriate. Please note that a violation of the Code or the Policy Statements may, under certain circumstances, also constitute a criminal act which may require the Company to start legal action against such violators or refer such violation to appropriate law enforcement authorities.

The Code and the Policy Statements identify conduct which is never acceptable and which will always be considered outside the scope of your employment. It is therefore crucial that each Employee read and understand the information presented in this Code and in the Policy Statements.[1]

[1] To assist Employees in complying with these principles, more detailed policy statements on some of the topics addressed below may be set forth in your Employee Handbook, as may be amended from time to time. In the case of any apparent conflict with the Employee Handbook, please seek guidance from the appropriate Compliance Officer.

SCOPE

The Code and the Policy Statements apply to all directors, officers and employees of the Company ("Employees"). In addition, where appropriate, affiliates and agents of the Company also may be required to comply with the Code and Policy Statements.

RESPONSIBILITIES

It is the responsibility of each Employee to conduct himself or herself in a manner that will support and maintain the Company's reputation for fairness and a high level of integrity. As representatives of the Company, it is essential that Employees' actions are legal and ethical. It is equally important that no actions taken by an Employee appear to others to be inconsistent with that high standard. In every case, an Employee should ask himself or herself if the conduct being contemplated would comply with Company policies and would withstand public disclosure and scrutiny. By doing business in this manner, we can ensure the respect of our clients, shareholders, fellow Employees, regulatory authorities, governments and neighbors.

ACKNOWLEDGMENT AND CERTIFICATION

The Code and Policy Statements supersede any pre-existing policy statement covering the same or similar subject matter. Every Employee must sign a Certificate of Compliance certifying that he/she has received and understands the Code and the Policy Statements and agrees to comply therewith. The required Certificate of Compliance, which must be signed and returned to the Group Compliance Officer or his/her designee, accompanies this document.

THE COMPLIANCE AND ETHICS PROGRAM

Overall responsibility for the functioning of the Company's Compliance and Ethics Program has been assigned to the Chief Financial Officer of ACGL, who functions as the Director of Compliance. The Director of Compliance may consult with other personnel as deemed appropriate and necessary to ensure the proper functioning of the Compliance and Ethics Program. Reporting to the Director of Compliance will be the Group Compliance Officers for each of the Company's operating groups. It is the Company's policy that each Employee be provided with the names, addresses, titles, telephone numbers and e-mail addresses of each of these persons.

QUESTIONS AND REPORTING

If you see any actual or proposed business conduct by an Employee or anyone doing business with the Company, which you in good faith believe constitutes a violation of the Company's Code, Policy Statements or any applicable law or regulation, or if you have any questions in that regard, or if you are aware of situations which could implicate the Company in unlawful conduct by others, you have an obligation and you are encouraged to come forward. When in doubt, ask before you act. You may bring any question you may have or report any questionable conduct to the Director of Compliance or your Group Compliance Officer, or their designees, or take advantage of the Compliance Hotline which has been established by the Company. To the extent practicable under the circumstances, all reasonable steps will be taken to keep

confidential the identity of anyone reporting a violation. We assure you that your communications will be taken seriously and, if warranted, the matter will be investigated.

The Compliance Hotline will record all calls and it is the responsibility of the appropriate Group Compliance Officer who will, as necessary, consult with the Director of Compliance, to determine what action, if any, is appropriate. Calls to the Compliance Hotline may be made anonymously if desired. It is the Company's policy that each Employee be provided with the telephone number of the Compliance Hotline.

The Company will protect Employees from negative consequences that may result from fulfilling their reporting obligations. The Company will not discharge, suspend, demote or take adverse employment action against an Employee who believes and communicates in good faith that a policy or practice is in violation of applicable laws, rules or regulations simply because an Employee makes any such report, unless the Employee has been a willful participant in the wrongdoing, has allowed or encouraged the violation to occur or has otherwise committed misconduct. This policy is intended to encourage Employees to come forward and report violations. We encourage Employees to disclose their own violations of any applicable law, regulation or Company policy. While we cannot promise in advance that Employees who report their own violation of any applicable law, regulation or ethical standard will not be disciplined or otherwise dealt with by appropriate authorities, we would apply any discipline in a fair and equitable manner.

TRAINING

To ensure that all Employees understand their responsibilities under the Code and Policy Statements, the Compliance and Ethics Program requires that the Director of Compliance, or his/her designee, and the Group Compliance Officers shall develop training programs to facilitate compliance with the Code and Policy Statements. New Employees will receive an introductory briefing on the principles of the Code and the Policy Statements as part of their orientation. All Employees whose responsibilities involve compliance with the laws, regulations or standards of conduct applicable to our operations will receive additional specialized training, including participation in periodic training sessions.

PROCEDURES REGARDING WAIVERS

Because of the importance of the matters involved in this Code and Policy Statements, waivers will be granted only in limited circumstances, where the circumstances would support a waiver and to the extent permitted by applicable local law and regulations. Waivers of the Code or Policy Statements may be made only by the Director of Compliance and the General Counsel of Arch Capital Services Inc. who may act individually or together. However, waivers of the Code or Policy Statements for executive officers or directors of ACGL may only be made by the Board of Directors of ACGL. Any waiver granted to the executive officers or directors of ACGL must be publicly disclosed on ACGL's website or on Form 8-K to the extent required by U.S. securities laws or the rules and regulations of any exchange applicable to us.

1. HONEST AND FAIR DEALING

Employees must endeavor to deal honestly, ethically and fairly with the Company's customers, suppliers, competitors and Employees. No Employee should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair dealing practice.

Unfair dealing is not only unethical but, in some circumstances, such conduct may rise to a level of fraud and thereby expose Employees and the Company to criminal and/or civil liability for violation of anti-fraud laws, as well as the antitrust laws. For example, prosecutors and private civil litigants have alleged fraud and other claims in connection with the submission by carriers of sham coverage quotes that reflect higher premiums and/or less favorable terms and conditions than the quotes submitted by the incumbent carriers, where the non-incumbent carriers' quotes were knowingly provided to assist the incumbent carriers in retaining the clients' business.

2. CONFLICTS OF INTEREST

Each Employee owes a duty of loyalty to the Company. For that reason, all Employees must exercise great care any time their personal interests conflict with those of the Company. Conflicts of interest are to be scrupulously avoided and, if unavoidable, must be disclosed by Employees at the earliest opportunity. A conflict of interest exists if your actions as an Employee are, **or could reasonably appear to be**, influenced, directly or indirectly, by personal considerations or by actual or potential personal benefit or gain. Employees should also comply with any conflicts of interest requirements which may be legislated in local law.

Employees, without authorization from the Director of Compliance or his/her designee, may not have a significant financial interest in any organization conducting or seeking to conduct business with the Company in a manner which is more than merely incidental or immaterial. A significant financial interest is one which is so substantial as to create a potential risk of interference with such individual's independent exercise of judgment in the interest of the Company. Employees who deal with the Company's suppliers are placed in a special position of trust which requires great caution. No Employee should ever receive a payment or anything of value in exchange for a purchasing decision, except for normal business entertainment and tokens of limited value, and in compliance with Section 3 of this Code.

No Employee of the Company shall participate on behalf of the Company in any negotiations or dealings of any sort with any person, firm, or non-affiliated corporation in which he/she has, directly or indirectly, an interest, whether through a personal relationship which would affect his or her decisions, or through stockholding or otherwise, except an ordinary investment not sufficient to in any way affect his/her judgment, conduct, or attitude in the matter, or give him/her a personal interest therein.

No Employee shall knowingly compete or aid or advise any person, firm, or corporation in competing with the Company in any way, or engage in any activity in which his/her personal interests in any manner conflict, or might conflict, with those of the Company.

The Company requires the full attention of its employees. In general, this level of attention makes it impractical for employees to pursue employment outside the Company. Additionally, outside employment also could lead to a conflict of interest for the employee.

The same conclusion applies to an employee or officer of the Company serving on the Board of Directors of another company. Consequently, any outside employment or holding the position of director of another corporation by any employee or officer must be approved in advance by the Director of Compliance, or his/her designee. This requirement shall not apply to an employee's or officer's holding the position of director of a not-for-profit entity. However, any non-employee director of the Company must notify the Board of Directors of the Company in the event that he or she holds the position of director of another for-profit entity.

Unless expressly authorized or sponsored by the Company, no outside activities should involve the use of the Company's time, name, influence, assets, funds, materials, facilities or employees.

Employees are prohibited from diverting for personal gain any business opportunity from which the Company might profit unless the Company validly decides to forego the opportunity. You must direct all questions regarding this subject to the Director of Compliance, or his/her designee.

3. ENTERTAINMENT, GIFTS AND PAYMENTS (NON-GOVERNMENTAL AND GOVERNMENTAL PERSONNEL)

The Company and any persons acting on its behalf, will procure goods and services and will sell its products and services on an impartial basis, free from outside influence. Business transactions should always be free from even a perception that favorable treatment was sought, received or given as the result of furnishing or receiving any financial or other advantage, including gifts, favors, hospitality, entertainment or other similar gratuity.

Any financial or other advantage, including payments or things of value, directly or indirectly, to any director, officer, employee or representative of any actual or prospective customer or supplier of the Company, given for the purpose of influencing or affecting such person's business judgment or action, such as to induce the purchase or sale of goods or services, or to induce them to act improperly in any way, is strictly prohibited. The competitive appeal of the Company's services and products must be based on their quality, price and other legitimate attributes recognized in the marketplace.

Non-governmental personnel

Employees, or any person acting on behalf of the Company, shall not seek or accept any financial or other advantage, including personal gifts, payments, fees, services, valuable privileges, vacations, or pleasure trips without a business purpose, loans (other than conventional loans from lending institutions), or other favors from any person or business organization that does or seeks to do business with, or is a competitor of, the Company. No Employee shall accept anything of value in exchange for referral of third parties to any such person or business organization.

Notwithstanding the previous paragraph, gifts to or from non-governmental personnel with whom the Company does or seeks to do business should not exceed U.S. $400 or any other lesser amount prescribed by local law per person or entity in a calendar year. Employees should make good faith estimates of the value of gifts which they receive. In any case where an Employee receives a gift which is believed to be in excess of this limitation, the Employee should return the gift with a polite note explaining the Company policy. Employees may give such gifts provided receipt of gifts is not prohibited by the recipient's employer and, regardless of value, there is no intention to induce the recipient to act improperly in any way.

For this purpose "gift" does not include providing or accepting meals and entertainment of reasonable value motivated by commonly accepted business courtesies, provided such meals or entertainment would not likely cause favoritism or a sense of obligation to the donor or induce the recipient to act improperly. Lavish or excessive meals or entertainment, or meals or entertainment involving the same customer or supplier on a recurring basis, should be avoided.

It is difficult to promulgate a rule as to what is "reasonable" or what is "commonly accepted business courtesy" to cover all circumstances. Employees are urged to make good faith judgments. A good test is — would you be embarrassed if your giving or receiving meals or entertainment were the subject of an article in the Wall Street Journal? In all matters, but particularly in cases of giving or receiving gifts, Employees must be alert to federal or state prohibitions or prohibitions in jurisdictions outside the United States applicable to particular businesses or lines of insurance.

Governmental personnel

Gifts to governmental personnel, including public officials whether or not located in the United States, should not be made, regardless of value, unless cleared in advance with the appropriate Compliance Officer.

In the United States, there are stringent federal restrictions on the provision of gifts, meals and entertainment to government officials and advance approval from the Director of Compliance or his/her designee is required. There are similar restrictions in numerous states and you must consult with the Director of Compliance or his/her designee in advance of providing gifts, meals and entertainment to governmental officials.

In jurisdictions outside the United States, gifts may not be provided to government officials without the express approval of the Director of Compliance or his/her designee. Meals and entertainment may be provided to government officials only if permissible under the host country laws and the laws of the country (subject to any legislated amounts permitted in local law) in which the Employee who offers such meals or entertainment is located, and the meals and entertainment must be modest in nature and not provided on a recurring basis.

Violations of this prohibition anywhere in the world may subject the Company and any involved Employees or agents of the Company to severe penalties under the laws of the United States, the United Kingdom and many other jurisdictions in which the Company does business.

You are urged to consult with the Director of Compliance or his/her designee if you have any questions regarding this policy.

4. PROTECTION OF PROPRIETARY AND CONFIDENTIAL INFORMATION AND PRIVACY

Proprietary information, that is, nonpublic information which if disclosed outside the Company could disadvantage the Company competitively or financially or which could hurt or embarrass Employees, customers, insurance claimants, suppliers or the Company, must be kept confidential. In addition to maintaining the confidentiality of our own proprietary information, our policy is to respect the proprietary information of others. Indeed, the theft of another's proprietary information is a crime in most jurisdictions.

It is the Company's policy that each Employee be provided with the Company's "Policy Statement on Insider Trading and Confidential Information." Employees are strongly urged to read such policy in its entirety and to consult with the General Counsel of Arch Capital Services Inc. in the event an Employee has any questions concerning the policy.

The Company's services reach deep into the personal and business lives of others, who trust us to protect their privacy. Violating that privacy may result in serious criminal charges, regulatory fines and civil liability for both the Company and the Employee responsible. It is the Company's policy to collect and process all personal data in accordance with the applicable privacy laws in each relevant jurisdiction. Every Employee should do his/her utmost to protect the privacy of all forms of business communications, whether voice, data or image transmissions. The United States, Canada and numerous European countries have adopted regulations to ensure the confidentiality of personally identifiable financial and other information. In the EU, the General Data Protection Regulation ("GDPR") is a significant new data privacy law which went into effect on May 25, 2018. As well as applying to the processing of all "personal data" by Arch entities established in the EU, it also has extra-territorial effect, to the extent that: (i) non-EU Arch entities provide services to data subjects in the EU; (ii) non-EU Arch entities provide products or services to consumers based in the EU; or (iii) non-EU Arch entities monitor the behavior of individuals in the EU (e.g. in the context of employee monitoring or website tracking). In the UK, the GDPR will continue to be effective through national implementing law following the UK's exit from the EU in March 2019.

In the United States, financial institutions may not disclose such information to a non-affiliated third party unless the institution has clearly disclosed to the individual that such information may be disclosed and is provided an opportunity, in advance of the disclosure, for the individual to direct that the information not be disclosed to a third party. Notice of the policies and practices with respect to disclosure shall be provided at the time of establishment of the relationship and annually during its continuation.

The Company policy is that personal data should be processed only by Employees who need the data to perform their jobs and in accordance with any local data protection laws and regulations. Personal data that is no longer needed should be destroyed consistent with record retention policies as may be adopted from time to time. In some jurisdictions, personal data may be transferred only in limited circumstances, for example upon consent, or if consent may be presumed based on the circumstances or if required or permitted to do so by law. Some jurisdictions, including all EU jurisdictions, impose restrictions on the cross-border transfer of personal data, which may need to be overcome with specific exemptions (such as an exemption for the obtaining of legal advice) or data transfer mechanisms such as standard contractual clauses or (in relation to transfers to the United States) the EU-US Privacy Shield scheme. Any Employee who receives an inquiry from any party outside the Company seeking nonpublic information regarding the Company, its Employees, customers, insurance claimants or suppliers must refer such inquiries to the Group Compliance Officer, the Director of Compliance or their respective designees.

Many countries, territories and states have data breach laws which require a regulator to be notified in the event of a breach of personally identifiable information, health or financial information. In the EU, the GDPR mandates notification of a "personal data breach" to the relevant supervisory authority within 72 hours of becoming aware of the breach. It is therefore imperative that any suspected loss, theft, misuse, damage to or destruction of records containing personal data (whether electronic or paper copy) it reported to your local IT manager, Arch Technology Services (securityoperations@archcapservices.com) or the Arch Group Data Protection Officer (ArchDPO@archcapservices.com).

5. INTEGRITY OF RECORDS, ACCOUNTING PROCEDURES AND DOCUMENT RETENTION POLICY AND PROCEDURES

Accuracy and reliability of our financial and business records is critically important to the Company's decision-making process and to the proper discharge of its financial, legal and reporting obligations. The Company's records must be honest, accurate and complete and must fairly represent the facts. The knowing or deliberate falsification of any documents may be the basis for immediate discharge and may subject an Employee to civil and criminal sanctions as well.

The Company follows the accepted accounting rules and controls as set forth by the Securities and Exchange Commission and the Financial Accounting Standards Board and the accounting practices prescribed or permitted by regulatory authorities as well as the applicable local accounting rules and principles. All account books, budgets, project evaluations, expense

accounts and other data papers utilized in maintaining records of the Company's business must accurately reflect the matters to which they relate. Without limiting the foregoing, all reports and documents filed with the Securities and Exchange Commission, as well as other public communications, should be full, fair, honest, timely, accurate and understandable. All assets of the Company must be carefully and properly accounted for. No payment of funds of the Company shall be approved or made with the understanding that any part of the funds will be used in a manner contrary to this principle.

Dishonest reporting of information to organizations and people inside or outside the Company, including false or artificial entries in books and records, is strictly prohibited. It could lead to civil or criminal liability for you and the Company. This includes not only reporting information inaccurately but also organizing it in a way that is intended to mislead or misinform those who receive it. No undisclosed or unrecorded funds or assets shall be established for any purpose. In a case where the Company permits petty cash funds to exist, such funds must be administered pursuant to the Company's system of internal controls.

The Company's independent registered public accountants shall be given access to all information necessary for them to conduct audits properly. Employees must not, and must not direct others to, take any action to fraudulently influence, coerce, manipulate or mislead any public or independent registered public accountant engaged in the audit or review of the Company's financial statements for the purpose of rendering those financial statements materially misleading; nor may they take any such action at the direction of any Employee. Examples of actions that could result in rendering financial statements materially misleading include: issuance of a report on the Company's financial statements that is not warranted in the circumstances due to material violations of generally accepted accounting principles, generally accepted auditing standards or other standards; non-performance of audit, review or other procedures required by generally accepted auditing standards or other professional standards; failure to withdraw an issued report under appropriate circumstances; and failure to communicate matters to the Company's audit committee. Any such actions will be deemed to be "for the purpose of" rendering the financial statement misleading if the person involved knew or was unreasonable in not knowing that the improper influence, if successful, would result in rendering financial statements materially misleading.

Business, tax, financial reporting and legal considerations require the orderly retention of Company records. For this purpose the Company has in place a Policy Statement on Record Retention which applies to electronic as well as paper records. All Employees must comply with this Policy, and Employees are urged to familiarize themselves with the Policy. The retention periods set forth in the Policy govern all Company records unless a directive has been issued by the Company advising that the purging of all or certain categories of documents has been suspended (for example, because of an imminent, threatened or pending government or regulatory investigation or proceeding, a pending civil litigation or proceeding, a subpoena or the like) until further notice. If any Employee believes that any records should be preserved beyond the prescribed period, for any reason (for example, because of knowledge of an imminent or

threatened investigation or proceeding), advice should be sought immediately from the office of the General Counsel of Arch Capital Services Inc.

It is the Company's policy that each Employee be provided with the Company's "Policy Statement on Record Retention."

6. E-MAIL/PC/ELECTRONIC COMMUNICATIONS

All computer hardware and software and other equipment, such as electronic devices, including but not limited to cell phones, smart phones, personal digital assistants, personal communications devices, flash drives/memory sticks, external hard drives and tablets, provided to Employees by the Company (hereinafter "Equipment"), as well as any information or data transmitted by or stored in such systems or Equipment (including electronic mail), are Company property and should be used primarily for business purposes. Equipment shall also include personal devices not owned by the Company to the extent used for Company business. Limited personal use, consisting of occasional personal e-mails or other communications and occasional personal Internet access is permitted, but the standard of reasonableness should govern. Thus, extensive personal use of the Internet as well as extensive use of the computer system or other Company Equipment for personal e-mail or other communications are forbidden. Notwithstanding that limited personal use is permitted, the Company reserves the right to monitor and inspect all electronic media, and all communications and data received, sent or downloaded using Equipment on a continuous and ongoing basis or from time to time. The monitoring or inspection of personal devices used for Company business must, however, be based on grounds to investigate suspected misuse or involve a legitimate business interest. Employees should not have any expectation of privacy when using these facilities or Equipment unless otherwise required by law. Any monitoring of emails or other forms of communication will be conducted in accordance with local legal and regulatory requirements. Employees should not participate in any on-line forum where the business of the Company or its customers or suppliers is discussed due to the possibility of violating the Company's confidentiality policy or subjecting the Company to legal or regulatory action for defamation or privacy violations, with the exception of participation in discussions about work-related issues that are protected under the National Labor Relations Act or any other applicable labor laws or regulations. The Company's e-mail system or other Equipment used for Company business may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations. It may not be used to create any offensive or disruptive messages, such as messages which contain sexual implications, racial slurs, or offensive references to race, color, religion, creed, sex, national origin, ancestry, disability, age, genetic information, citizenship status, pregnancy, gender identity or expression, affectional or sexual orientation, atypical cellular or blood trait, marital status, veteran status, membership in the armed services, political affiliation, any other characteristic protected by applicable law, or in any other way which may involve or lead to a breach of this Code or of any applicable laws or regulations.

It is the Company's policy that each Employee be provided with the Company's "Policy Statement on Use of the Company's Computer Network, Including E-Mail Communications."

7. POLITICAL CONTRIBUTIONS AND INVOLVEMENT IN POLITICAL ACTIVITIES

No contributions, expenditures or other financial assistance, including loans, will be made by or provided on behalf of the Company, directly or indirectly, to political candidates, causes or parties, including through charitable donations, except with the approval of the Board of Directors and in accordance with applicable law. Employees are encouraged to vote and participate fully in the political process. Employees who participate in partisan political activities must make every effort to ensure that they do not give the impression that they speak or act for the Company. Any Employee's personal political contributions cannot be reimbursed by the Company, directly or indirectly.

When dealing with public officials, Employees must avoid any activity that is, or is likely to be perceived as, illegal or unethical, or that reflects a favoritism not accorded to others. The appearance of impropriety is as damaging to our Company as an actual misdeed. Employees must exercise caution to prevent relationships and dealings with public officials from becoming subject to question.

In the event that the Company or any subsidiary of the Company enters into a contract with the State of Connecticut legislative or executive branches or any quasi-public agency of the State or submits a bid or holds a valid prequalification certificate issued by the State, the General Counsel of Arch Capital Services Inc. should be promptly notified. In such event the General Counsel will provide guidance regarding the prohibitions imposed by the State on state contractors which include prohibitions on contributions to candidates for specific offices and contributions to their political committees, by "principals" of state contractors whose contracts or bids meet certain financial thresholds as well as prohibitions on soliciting contributions from the contractor's employees or subcontractors. The prohibitions cover, among others, members of the Board and officers and employees having managerial or discretionary responsibilities to administer the state contract, as well as spouses and dependent children.

8. ANTITRUST AND COMPETITION

The global activities of the Company are subject to antitrust and competition laws of various countries. Employees are required to consult with the General Counsel of Arch Capital Services Inc. on all antitrust-sensitive matters. Antitrust violations can generate civil liability and the risk of substantial fines being imposed on the infringing entity and/or members of its corporate group. In many jurisdictions, antitrust violations also carry possible criminal sanctions, punishable by large fines and the potential incarceration of responsible Employees. Employees responsible for antitrust violations can also be disqualified from serving as directors of a company. In many jurisdictions, victims of antitrust violations can bring private damages claims to seek compensation for the harm they have suffered as a result of the violation.

Some enforcement agencies worldwide may offer amnesty to those who first report violations. Amnesty and/or a significant reduction in fines may also be available to the Company if it cooperates with the relevant antitrust regulators. Thus, suspected problems should be brought to the attention of the General Counsel of Arch Capital Services Inc. without delay.

In general, antitrust and competition laws prohibit understandings, agreements or actions that may restrain trade or reduce competition. Violations include agreements among competitors or others to fix or control prices, rig bids or to allocate territories, markets or customers, or abuse of a dominant position. It is important to recognize that customers (including some brokers) may also be competitors, even when they sell products as agent for the Company. Exceptions may exist for lawful joint ventures or regulated activities in certain countries. Employees must have the express consent of the General Counsel of Arch Capital Services Inc. before relying on any such exception.

The Company prohibits Employees from unlawfully restraining trade or reducing competition. This includes participating in any direct or indirect discussions or other communications, understandings or agreements with, or for the benefit of, a competitor regarding for example:

- Premiums, rates, commissions or prices;
- Matters that would affect the availability or terms of insurance or reinsurance coverages or of other services or products;
- Allocation of markets, territories or potential insureds, reinsureds or other customers;
- Limiting the number of insurers competing to sell insurance;
- Encouragement of a boycott of an insurance product or service or any other product or service, including whether to quote or not to quote certain types of classes or risks;
- What constitutes a “fair” profit level; or
- Credit terms.

Industry exchanges of price data or other commercially sensitive information must strictly comply with legal requirements and should not be undertaken without approval of the General Counsel of Arch Capital Services Inc. Participation in insurance and reinsurance pools must also strictly comply with legal requirements, particularly in the European Union.

Employees are also prohibited from discussing with or providing to any competitor, insurance broker or other third party (directly or indirectly) any artificially inflated bids, prices and/or other terms and conditions with respect to insurance or reinsurance in order to lessen competition by, for example, conferring a commercial advantage upon a third party and/or creating a false appearance of legitimate competition.

9. SECURITIES TRADING

It is the Company's policy that each Employee be provided with the Company's "Policy Statement on Insider Trading and Confidential Information." Employees are strongly urged to read such policy in its entirety and to consult with the General Counsel of Arch Capital Services Inc. in the event an Employee has any questions concerning the policy.

10. ANTI-BRIBERY AND CORRUPTION

The Company will not engage in bribery or corruption in any form (whether it involves private individuals or government officials) and has a zero tolerance approach to violations.

The Company prohibits any Employee of the Company, or any person acting on behalf of the Company (an "associated person"), such as an agent or representative, from directly or indirectly requesting, accepting, soliciting, agreeing to receive, promising, offering or giving a bribe (which includes facilitation payments, kickbacks or any other improper payments or financial advantages) to any person.

The Company prohibits any Employee or any associated person acting on behalf of the Company from offering, paying, promising to pay or authorizing the payment of money or anything of value, directly or indirectly, to an officer or employee of a government (including a state-owned commercial entity), legislative, administrative, public or judicial body, political party, party officials, candidates for political office and officers or employees of public international organizations with the intent or purpose of obtaining, retaining or directing business, a concept which is broadly construed to include seeking any commercial advantage.

All of the Company's activities must be managed in full compliance with the Code and all applicable legal and regulatory anti-bribery and corruption obligations, including the U.S. Foreign Corrupt Practices Act and The UK Bribery Act.

Violations of this prohibition may subject the Company and any involved Employees or associated persons of the Company to severe civil and/or criminal penalties under the laws of the United States, the United Kingdom and many foreign jurisdictions in which the Company does business. Any known or suspected bribery or corruption problems should be brought to the attention of the Director of Compliance or his/her designee without delay.

11. COPYRIGHTS

Copyright laws protect original creative expression in a number of forms, including written materials, software and the like, and prohibit their unauthorized duplication and distribution. Employees are prohibited from reproducing, distributing or altering copyrighted materials from books, trade journals, computer software, magazines, tapes, disks, videotapes or online content without permission of the copyright owner. Using unlicensed software could consti-

tute copyright infringement. The Company subscribes to a number of trade journals and magazines and Employees must take particular care to avoid copying portions of these materials for distribution to others.

Employees should assume that creative works developed by them in the course of performance of their duties are the property of the Company unless they are formally advised otherwise in writing. Questions on this subject should be addressed to the Director of Compliance or his/her designee.

12. POLICY AGAINST DISCRIMINATION AND HARASSMENT

The Company is committed to providing equal employment opportunities to all Employees and prospective Employees in every facet of its operations. All employment-related decisions, including hiring, employee treatment, training, compensation, promotion, transfer, benefits and disciplinary action, are made solely on the basis of the individual's job qualifications and performance, and without regard to race, color, religion, creed, sex, national origin, ancestry, disability, age, genetic information, citizenship status, pregnancy, gender identity or expression, affectional or sexual orientation, atypical cellular or blood trait, marital status, veteran status, membership in the armed services, political affiliation, or any other characteristic protected by applicable law.

Sexual harassment, as well as any other form of harassment prohibited by law, is unacceptable and will not be tolerated. The Company will investigate all complaints of harassment and take remedial action as warranted under the circumstances. Behavior constituting harassment on any basis prohibited by law will be treated with the utmost seriousness and may result in disciplinary action, including immediate termination of employment. Conduct of this type engaged in by contractors, vendors and clients toward Company Employees will similarly not be tolerated.

No individual who raises a concern regarding a violation of the Company's policies against discrimination or harassment will be penalized or otherwise retaliated against.

It is the Company's policy that each Employee be provided with the Company's "Policy Statement Against Discrimination and Harassment."

13. ALCOHOL AND DRUGS

The Company requires a workplace which is free of alcohol and drugs and which complies with laws governing controlled substances. Anyone who is on the job under the influence of alcohol or, without medical authorization, any controlled substance is subject to disciplinary action, including immediate termination of employment.

Unless part of a Company-sponsored social event or business-related lunch or dinner, consumption of alcohol on the premises of the Company is prohibited; violation of this policy will subject an Employee to disciplinary action, up to and including immediate discharge.

The possession, use, sale, distribution or manufacture on Company premises of illegal drugs or non-medically authorized controlled substances is prohibited and will subject an Employee to disciplinary action, including immediate termination of employment.

The Company, in its discretion, reserves the right to randomly test Employees for the use of alcohol or other controlled substances, unless prohibited by applicable law.

14. PROTECTING OUR ENVIRONMENT

The Company is committed to protecting and improving the environment in all areas of the Company's operations, thereby preserving and enhancing the quality of life of our Employees, customers and neighbors. This commitment is a shared responsibility with all Employees.

15. SAFETY

The Company strives and is committed, so far as is reasonably practicable, to providing its Employees with a healthy and safe environment.

The Company is committed to providing the best possible working conditions for its Employees. The place of employment is to be free of recognized hazards that might cause injury or death as well as be in compliance with specific safety and health standards.

All Employees have the responsibility to their fellow Employees and to the Company to carry on their duties in a safe and efficient manner. Employees must report any unsafe conditions and immediately correct any unsafe acts observed or performed.

16. RETENTION OF AGENTS AND REPRESENTATIVES

Agents and representatives cannot be used to circumvent the law or this Code. All agents and representatives should possess the requisite business ethics required by the Company and therefore due care, skill and diligence shall be used when appointing any agent or representative. Any questions in this regard should be directed to the Group Compliance Officer or his/her designee.

17. ANTI-BOYCOTT

Laws and regulations implemented by the United States contain a broad range of sanctions directed at U.S. companies (including foreign entities controlled by domestic entities) which participate in boycotts of other countries which are not approved by the United States (for example, the Arab boycott of Israel). Violations of regulations implemented by the U.S. Department of Commerce, including failure to report receipt of boycott-related requests such as requests for information concerning relations with blacklisted companies, can subject violators to substantial civil and criminal penalties. Regulations implemented by the U.S. Department of the Treasury subject taxpayers to loss of tax credits for agreeing to participate in a non-sanc-

tioned boycott. All Employees shall refer any request to participate in any non-sanctioned boycott to the Group Compliance Officer or his/her designee. The foregoing applies to persons and entities that are subject to U.S. laws.

18. PROHIBITIONS ON FINANCIAL TRANSACTIONS INVOLVING DESIGNATED COUNTRIES, ENTITIES AND PERSONS

Many of the countries in which the Company transacts business, including the United States, the member states of the European Union (including the United Kingdom), Switzerland and Canada, have enacted prohibitions against financial transactions involving designated countries, or persons or entities acting on their behalf (known in the United States as "Specially Designated Nationals" or "SDNs"). Specially Designated Nationals or SDNs or other restricted parties may be found anywhere in the world, including within the United States or Europe. **NOTE: This area of the law is subject to change at any time due to the political nature of economic sanctions; thus, if there are any material changes to relevant sanctions laws, this section will be superseded by updates from the General Counsel.**

United States restrictions include an embargo prohibiting most financial transactions between persons and entities subject to the jurisdiction of the United States and Iran, subject to very limited exceptions for humanitarian items such as food and medicines. Persons and entities subject to these U.S. restrictions which are administered by the Office of Foreign Assets Control ("OFAC")of the U.S. Department of Treasury are: U.S. citizens and residents; persons within the U.S.; entities organized under the laws of the U.S. or any state of territory; any entity owned or controlled by U.S. persons or entities. Foreign persons who are determined to have violated the United States statutory prohibitions with regard to dealings with Iran are subject to the imposition of separate sanctions (beyond any OFAC designations) by the Department of State.

The U.S. sanctions pertaining to Iran are in a state of flux. Under the Joint Comprehensive Plan of Action (JCPOA or Iran Nuclear Deal), implemented on January 16, 2016, varying degress of sanctions relief were put into effect in the United States, the European Union, and the United Nations. The JCPOA did not contemplate the lifting of all sanctions against Iran, and those which were modified have the possibility of immediate "snap back" into place should Iran's compliance fail to meet the requirements of the agreement.

The U.S. and EU have taken different approaches regarding Iran's compliance with the JCPOA. The EU currently stands by the Iran Nuclear Deal and has afforded some sanctions relief. All EU economic and financial sanctions made in connection with the Iranian nuclear program have been lifted and new opportunities to engage in transactions involving Iran have opened up. Nonetheless, there remains a misconception that the JCPOA lifts all EU sanctions imposed on Iran - the Company will need to continue to comply with certain EU licensing obligations, prior authorization requirements, continued asset freezing provisions and wider EU human-rights and antiterrorism-related sanctions which remain in place against Iran. In the event of Iran not meeting the on-going commitments of the JCPOA, the EU will reintroduce sanctions.

In contrast, the U.S. government declared on May 8, 2018 that it was withdrawing from the Iran Nuclear Deal. This decision has no impact on primary U.S. sanctions that have remained in effect all along: as set forth above, U.S. persons are generally not able to do business in or with Iran unless authorized by OFAC. The U.S. announcement does affect the secondary sanctions relief that had been afforded non-U.S. persons such as foreign subsidiaries of U.S. companies who complied with special licensing procedures under OFAC's General License H. OFAC announced that it is withdrawing General License H and will replace it with wind-down licenses to allow companies a period of time to wind-down and exit any previously allowed Iranian business before Iranian sanctions "snap back". The Company is currently examining its previous business entered into under General License H and winding down any business as required. Arch is also reviewing and plans to rescind its Recusal and Operations Policy Consistent with General License H in due course with the formal elimination of General License H. U.S. law also mandates the public disclosure in SEC filings of certain dealings by the Company and any of its affiliates with the Government of Iran, or with Iran, or with specified SDNs. Because sanctions pertaining to Iran are subject to change, employees should monitor the OFAC website and consult Company counsel for the latest updates.

United States restrictions also include an embargo prohibiting most financial transactions between persons and entities subject to the jurisdiction of the U.S. and Cuba and its nationals (however blocking legislation prohibiting compliance with the U.S. prohibitions may apply in the United Kingdom, the European Union, Switzerland, Canada and elsewhere). Persons and entities subject to the U.S. restrictions are: citizens or residents; persons within the U.S.; entities organized under the laws of the U.S. or any state or territory; any entity wherever organized or doing business owned or controlled by U.S. citizens or residents or by entities organized under the laws of the U.S. or any state or territory. The former Administration announced certain changes in U.S.-Cuba relations on December 17, 2014, and on July 22, 2015 the United States lifted the designation of Cuba as State Sponsor of Terrorism. The Cuba trade embargo remains in place and most transactions between the U.S. or persons subject to U.S. jurisdiction are still prohibited. The changes adopted are intended to increase engagement and empower the Cuban people by facilitating specific types of authorized travel to Cuba (but not tourism), certain authorized commerce, and increased flow of information to, from and within Cuba. New general licenses have been added to the regulations in support of these goals. In September 2015, OFAC and the Commerce Department's Bureau of Industry and Security (BIS) amended the Cuban Assets Control Regulations and Export Administration Regulations, respectively, easing travel and telecommunications restrictions and allowing certain persons to establish a physical presence in Cuba. OFAC and BIS announced amendments to the Cuban sanctions regulations that took effect on March 16, 2016 which expand Cuba and Cuban nationals' access to U.S. financial institutions and, coupled with other arrangements announced by the Departments of State and Transportation allowing scheduled air service and regular travel by ship, increase the ability of U.S. citizens to travel to Cuba, additional steps consistent with the policy changes previously announced. Insurers are allowed to provide travel insurance for authorized travel to Cuba. On June 16, 2017, the President announced changes to Cuban sanctions to eliminate certain people-to-people travel and to prohibit dealings with any firm controlled by

the Cuban military or its intelligence or security services. On November 8, 2017, new regulations were released to implement this new initiative.

The U.S. has enacted additional restrictions which do not apply to foreign entities owned or controlled by U.S. entities or persons, but which do apply to the other persons and entities listed above. U.S. persons (excluding foreign entities owned or controlled by U.S. persons) are prohibited from insuring any vessel flagged by North Korea. Executive Orders issued in March 2016 and September 2017 imposed additional sanctions on North Korea. These Executives Orders added individuals, entities and vessels to the North Korea sanctions, prohibit the exportation of goods, services and technology to North Korea, prohibit new investment in North Korea, impose additional designation criteria for imposing blocking sanctions based on specific dealings with North Korea, and authorize the imposition of "secondary sanctions," which would effectively prohibit foreign financial institutions that conduct business or facilitate transactions with North Korea from access to the U.S. financial system. Property has been blocked and certain persons, entities and industries have been designated under these sanctions.

Congress passed legislation that was signed by the President in August 2017, codifying into law sanctions the former President implemented against Russia in response to the annexation of Crimea and alleged interference in the U.S. Presidential election. The law codifies designations as SDNs of individuals and entities that threaten the peace, security or stability of Ukraine. Certain of such persons are within the Russian Federation. The legislation expands the scope of existing "sectoral sanctions" that impose restrictions and prohibit financing for or otherwise dealing in new debt and equity for listed participants in specific sectors of the Russian economy—energy, banking, defense, railways and mining—as well as prohibiting the provision, exportation or reexportation to certain Russian energy companies of goods and services (other than financial services) by U.S. persons in support of specific types of Russian oil exploration and production, namely, deepwater, Arctic offshore and shale projects that have the potential to produce oil for Russia and in which designated Russian entities hold at least a 33% stake. In addition, the U.S. has imposed an embargo against transactions involving the Crimean region of the Ukraine. The law also requires the President to provide Congress at least 30 days' notice of an intent to repeal or relax Ukraine-related Russian sanctions, which can occur only with Congressional approval. Amid a further cooling of relations between Washington and Moscow, a number of high-profile Russian persons and entities were designated as SDNs in April 2018. This is a fast-moving situation that should be monitored closely, and further such designations are not unforeseeable.

There remains in place a significant embargo against transactions with Syria. Sanctions on Sudan were lifted in October 2017 in light of ongoing cooperation and engagement, though Sudan remains on the U.S. list of state sponsors of terrorism, and as such a general license is required for the export and reexport of certain items (commodities, software and technology). In April 2016, a new Executive Order was issued imposing new sanctions on individuals and entities that threaten the peace, security or stability of Libya. The Burma sanctions program terminated in October 2016.

The U.S. also blocks the assets of and prohibits transactions with Specially Designated Terrorists ("SDTs"); Foreign Terrorist Organizations ("FTOs"); Specially Designated Narcotics Traffickers and Kingpins ("SDNTs" and "SDNTKs"); certain designated transnational criminal organizations; persons and entities associated with the former Qadhafi regime; former Yugoslavia leaders; individuals and entities undermining democratic process in Zimbabwe, Belarus, the Western Balkans, or Lebanon; persons undermining the peace or stability of Iraq; persons constituting a threat to stability in the Democratic Republic of the Congo; and persons threatening the peace, security or the stability of Burundi, Somalia, Yemen, or the Central African Republic. Most transactions with the Government of Libya are authorized, subject to certain limitations. Transactions with the Palestinian Authority are restricted. In response to perceived violations of human and political rights, in August 2017, the President significantly expanded sanctions on Venezuela, which included restrictions on dealings with the government of Venezuela, including its state-owned oil company Petroleos de Venezuela, S.A., and Venezuelan access to U.S. capital markets. On March 19, 2018, by Executive Order, the financial sanctions were extended to any digital currency issued by the Government of Venezuala. There are also arms embargoes concerning certain countries and restrictions relating to trading in rough diamonds. Transactions involving exports or reexports to designated entities which have been found to have engaged in proliferation activities are also restricted. Regulations have been issued and designations of persons have been made to implement the cyber-related sanctions program, which targets persons responsible for cyber-enabled activities that result in harm to the national security, foreign policy or economic health or financial stability of the U.S. OFAC has issued regulations expanding U.S. sanctions and targeting Hizballah by authorizing the imposition of "secondary sanctions" against foreign financial institutions determined to be supporting the organization.

In addition to the United States restrictions, numerous other governments, including governments of member states of the European Union (including the United Kingdom), Switzerland, Australia and Canada, have adopted trade restrictions limiting transactions involving certain of the same persons, entities and countries as the U.S. economic sanctions referenced above. In addition, in some instances, these governments have imposed further financial sanctions, including against different persons and entities from the United States sanctions referenced above. Furthermore, pursuant to United Nations and European Union restrictions, hundreds of countries have imposed asset freezes on various terrorists and terrorist organizations.

On leaving the European Union in March 2019, the United Kingdom will maintain an autonomous sanctions regime. However, this is expected to mirror that of the European Union in the short to medium term, at least. Nevertheless, the Company should be vigilant for future divergence.

Because of the very serious consequences of violating these restrictions — civil and criminal penalties and likely damage to the Company's reputation — it is essential that Employees "Know Their Customers" and that thorough and frequent checks are made to ensure that transactions involving those customers are not restricted by applicable laws. A first step in finding information on these restrictions may be secured at the following websites:

- United States Treasury Department Office of Foreign Assets Control: https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
- United States Department of Commerce, Bureau of Industry and Security "Lists of Parties of Concern": http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern
- United Nations: https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
- European Union: http://eeas.europa.eu/cfsp/sanctions/index_en.htm
- United Kingdom: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets
- Canada: http://www.international.gc.ca/sanctions/index.aspx?lang=eng
- Australia: http://www.dfat.gov.au/un/unsc_sanctions/index.html
- Switzerland: https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos.html

19. MONEY LAUNDERING

All Employees must be vigilant in order to protect the Company from being unknowingly swept into a money laundering transaction. Money laundering is a term used to describe the process of integrating proceeds from illegal activities into the legitimate financial system so that the proceeds appear to have originated from a legitimate source. Transactions need not be cash transactions to constitute money laundering and money laundering can involve any movement of funds, cash or otherwise. Many countries, including the United States, Canada, Ireland, the United Kingdom and Bermuda, have adopted statutes which make participation in money laundering a criminal offense and subject the offender to harsh penalties.

Fundamental stages of money laundering include the placement or physical disposal of criminal proceeds into the financial system, followed by the creation of layers of transactions designed to obscure the source. Money laundering also includes use of the financial system to further international criminal activity.

Any Employee who knowingly permits illegal conduct or closes his or her eyes to suspicious activity that indicates possible money laundering will not only be subject to discipline by the Company, but may also subject himself or herself and the Company to criminal and civil penalties.

Money laundering issues are complex and you should not attempt to handle them on your own. If you become aware of any questionable circumstances, which could suggest money laundering, or if you have any questions, you must promptly consult the Group Compliance Officer or his/her designee.

The Company's program of vigilance to combat any attempt to use the Company's facilities to launder money consists mainly of the following elements:

1. Verification, or "Knowing Your Customer"
2. Maintaining documentation
3. Recognition and reporting of suspicious transactions
4. Training

The Financial Crimes Enforcement Network of the U.S. Department of the Treasury has promulgated regulations requiring that insurance companies that deal in "covered products" adopt anti-money laundering programs. "Covered products", which are those that present significant risk for money laundering, are:

- permanent life insurance policies, other than a group life insurance policy;
- annuity contracts, other than group annuity contracts; and
- any other insurance product with features of cash value or investment.

Other laws and regulations may apply to subsidiaries or branches of the Company located outside the United States, and Employees of those subsidiaries and branches of the Company must comply with any local requirements.

With respect to "covered products" the following steps must be undertaken in the United States:

1. Verification, or "Knowing Your Customer"

Most of the Company's customers are large, established corporations and institutions listed on recognized stock exchanges or subsidiaries of such companies and pose little risk of money laundering because of their financial transparency. For these customers, the preparation of standard account opening and transaction documentation would be sufficient verification, absent questionable circumstances.

In the case of customers less known or not known to the Company at all and companies not quoted on a recognized stock exchange or their subsidiaries, we must be satisfied that the customer is a legitimate entity engaging in a legitimate transaction and verification procedures must be undertaken. For example, steps should be taken to verify the customer's underlying beneficial owners, that is, those who ultimately own or control the customer (for example, those with interests of 5% or more). Individuals who seek to become customers and who are not known to the Company should be personally interviewed regarding the nature and history of their business. Accounts handled by an intermediary may present specific risks, particularly when the beneficial owners are not identified.

2. Maintaining documentation

The Company's policy is to retain for a minimum period of five years all documentation relating to the verification of the identity of the customer, as well as all records relating to each

transaction, in readily retrievable form. Such records must be maintained even after the customer relationship has been terminated.

3. Recognition and reporting of suspicious transactions

Once an account is opened, it must be monitored for any signs of money laundering. Suspicions must be reported to the appropriate Group Compliance Officer or his/her designee and you must not disclose this information to the customer. A suspicious transaction would include one that is inconsistent with a customer's known legitimate business or activities, one involving unusual payment methods or one involving early termination with the proceeds directed to a third party.

4. Training

The Company's training program, which is part of the Company Compliance and Ethics Program, will include training on money laundering. The Company may also give more specialized training to Employees whose duties could expose them to attempted money laundering, such as Employees responsible for the opening of new accounts, as well as the training of their superiors.

CODE OF BUSINESS CONDUCT (JUNE 2018)
ACKNOWLEDGMENT AND CERTIFICATE OF COMPLIANCE

I hereby certify that I have received, read and understand the Code of Business Conduct, including, without limitation, the Policy Statements attached thereto, of Arch Capital Group Ltd. and its subsidiaries, and agree to its terms and further agree that it is my responsibility to comply with all policies, guidelines and obligations contained therein.

I acknowledge and agree that this Code does not constitute an employment contract, nor a guarantee of continued employment with Arch Capital Group Ltd. or any of its subsidiaries. I understand that employees who violate the Code of Business Conduct may be subjected to disciplinary action, including possible termination of employment.

Signature: _____

Print Name: _____

Title/Position: _____

Date: _____

Return this certification no later than two weeks after receipt to your Group Compliance Officer or his/her designee for inclusion as part of your personnel file.

If there is any uncertainty as to the applicability of any principle or policy to a particular situation or the propriety of any contemplated course of action, the Director of Compliance or your Group Compliance Officer (or their designees) should be contacted for assistance and guidance. You may also take advantage of the Compliance Hotline which has been established by Arch.

Contact information for the Director of Compliance and the Group Compliance Officers and the Compliance Hotline telephone numbers have been provided to Employees.