# Stewart
# Code of Business Conduct and Ethics

stewart™

# Stewart Code of Business Conduct and Ethics

## Table of Contents

## Policy

### Introduction

This Stewart Code of Business Conduct and Ethics ("Code") has been adopted by Stewart Information Services Corporation's Board of Directors (the "Board") and is applicable to Stewart Information Services Corporation, Stewart Title Guaranty Company, Stewart Title Company and applicable Stewart Family of Companies (collectively "Stewart" or "Company"). This Code applies to every employee, officer and director of Company. For convenience, the term "Employee" is used throughout this Code as a designation that includes Company employees, officers and directors. Also, the term "Compliance Officer" means any of Chief Legal Officer, Chief Compliance Officer, Deputy Chief Compliance Officer, Deputy General Counsel, Chief Human Resource Officer, or other corporate compliance officer designated as such from time to time by a Compliance Officer or the Board. For Employees based outside the United States, the term "Compliance Officer" means the Chief Compliance Officer or any one of the applicable department heads of Human Resources, Legal and Regulatory Compliance in that region.

Operating with a strong sense of integrity is critical to maintaining trust and credibility with our policyholders, customers, employees, and shareholders. The Code is intended to provide information, support and resources to ensure that we act ethically and in compliance with the laws and regulations that affect our business. Adherence to this Code is vital for the Company to continue as a leader in our industry and to preserve the Company's reputation for honesty and strong ethical standards.

This Code outlines the broad principles of legal and ethical business conduct embraced by the Company. It is not a complete list of legal or ethical questions an Employee might face in the course of business and, therefore, this Code must be applied using common sense and good judgment. This Code may be supplemented with other corporate or divisional policies, and the Stewart Employee Policies, to address specific topics in additional detail including, but not limited to, Standards of Conduct, IT Security and Computer Usage, and Social Media and Media. Unless specifically indicated, such supplemental policies shall not be deemed to conflict with or supersede the provisions contained in this Code.

Additionally, under certain circumstances, laws and regulations may establish requirements that differ from this Code and the Company's policies may prohibit a broader range of conduct than what is required by law or regulation. Employees worldwide are expected to comply with this Code, all applicable laws, regulations and Company policies. Employees based outside the United States are subject to the relevant Schedule, if available, for their jurisdiction which contains region-specific laws, regulations and Company policies in accordance with this Code. In the event that there appears to be a conflict between the laws and regulations in a specific jurisdiction and Company policies, Employees must follow the jurisdiction-specific laws and regulations and notify the Company's Compliance Officers at ethics@stewart.com of the apparent conflict.

This Code is administered by the Chief Compliance Officer and may be amended or modified at any time by the Board. Employees will be notified of such changes as soon as reasonably practical. No Code of Conduct can anticipate or formulate in advance an all-inclusive set of guidelines regarding appropriate business conduct. If you have questions or concerns about this Code or about situations that are or are not specifically addressed by this Code, please consult with management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

*Reporting Violations and Potential Violations*

The Company encourages, and it is the responsibility of all Employees, to promptly report any instances which they believe may constitute violations or suspected violations of laws, rules, regulations, the Company's policies or this Code, including financial improprieties, ethical violations, or illegal activity (each, a "Violation"), regardless of whether such Violations or suspected Violations have been committed by Employees, vendors, contractors, consultants, customers or any other party having a business relationship with the Company. Employees should seek guidance from a Compliance Officer with any questions or concerns regarding a Code related matter and no one has the authority to instruct an Employee to violate this Code. Employees may report a Violation or suspected Violation, or report received instruction to violate this Code, to management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com. Reports may be anonymous, if so preferred. The Company will undertake an investigation and will endeavor to protect the privacy and confidentiality of all parties involved to the extent possible, consistent with a thorough investigation. Further information about reporting violations or EthicsPoint may be found on the Company's intranet site, StewartPoint. Employees should seek guidance from management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com. Please contact a Compliance Officer with any questions or concerns regarding a Code related matter or when in doubt about the best course of action in a particular situation.

Return to Top

*Investigations*

The Company's Legal Department, Compliance Department, or Human Resources Department may conduct investigations as they deem appropriate and necessary into suspected violations of this Code or any supplemental policy. Employees are required to cooperate fully with any investigation whether internal or external. Making false statements or otherwise making misleading statements to the investigators, whether internal or external, is cause for immediate termination of employment and may give rise to civil or criminal legal actions or penalties.

The making of a report does not mean a violation has occurred. The Company will investigate each concern, and the subject person will be presumed not to have violated this Code unless a violation is substantiated. The information collected for purposes of the investigation will be treated as confidential and will be shared only on a need to know basis.

*Retaliation*

Retaliation, retribution, or harassment against any Employee who, in good faith, asks any questions or raises any concern regarding this Code, cooperates in the investigation of a suspected or actual violation, or in good faith asks any questions or raises any concern regarding this Code is prohibited and is grounds for disciplinary action, up to and including termination of employment. "Good faith" does not mean that a reported concern must be correct, but it does require that the reporting person be truthful when reporting a concern or asking a question. If an Employee believes that someone who has made a report of a violation or suspected violation or who has cooperated in the investigation of a violation or suspected violation is a victim of retaliation or other adverse employment consequence, the individual should contact management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

No Code of Conduct can anticipate or formulate in advance an all-inclusive set of guidelines regarding appropriate business conduct. If you have questions or concerns about this Code or about situations that are not specifically addressed by this Code, please consult with management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

*Non-Interference*

Notwithstanding any other provision of this Code, nothing in this Code shall prohibit the Employee from confidentially or otherwise communicating or filing a charge or complaint with a federal, state, local or other governmental agency or regulatory (including self-regulatory) entity including concerning alleged or suspected criminal conduct or unlawful employment practices; participating in a governmental agency or regulatory entity investigation or proceeding; giving truthful testimony or statements or disclosures to a governmental agency or regulatory entity, or if properly subpoenaed or otherwise required to do so under applicable law; or requesting or receiving confidential legal advice at the Employee's own expense.

Furthermore, the U.S. Defend Trade Secrets Act of 2016 provides that: (a) an individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that (A) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney, and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (B) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal; and (b) an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual (A) files any document containing the trade secret under seal, and (B) does not disclose the trade secret, except pursuant to court order. Nothing in this Code prohibits or creates liability for any such protected conduct.

Return to Top

**Accounting and Financial Reporting**

The Company fully and fairly discloses the financial condition and results of operations in compliance with applicable financial reporting and accounting laws, rules and regulations. To meet its obligations, the Company relies on Employee truthfulness and a system of internal accounting controls to ensure the accuracy of its financial statements.

*Improper Payments*

Improper and/or excessive payments of any type from the Company to Employees, agents, consultants, professionals, or vendors are prohibited by this Code. If improper payments, or suspected improper payments, are identified, they must be reported to management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com. Examples of improper payments include, but are not limited to, the following:

- Payments for services not needed, not ordered, or not properly documented and substantiated;
- Payroll-related expenditures, bonuses, commissions, awards and noncash gifts given to or by Employees without proper approval and adequate documentation;
- Payments made in cash or checks drawn or payable to "Cash" or "Bearer";
- Payments made for any purpose other than a legitimate business purpose described in supporting documents;
- Payments made to employees of policyholders, customers or vendors, directly or through intermediary persons, entities or organizations, or that seem to deviate from normal business transactions;
- Conversion of Company funds or funds of a third party being held by the Company to or for personal use;
- Payment to or from an entity in which an Employee or Related Party has an undisclosed interest; and
- Use of escrow funds for any purpose other than as provided in properly authorized instructions given by the parties to the transaction and received by the Company.

## Adherence to Company Bulletins and Policies

All Employees shall review and comply with the Company's various bulletins and policies as published, disseminated and updated from time to time. These policies can be located in Virtual Underwriter and/or on the Company's intranet site, StewartPoint.

## Antitrust

The Company's success depends on building productive relationships with customers, suppliers, vendors, competitors, and Employees based on integrity, ethical behavior, and mutual trust. As such, each Employee should deal fairly with the Company's customers, suppliers, vendors and competitors. Taking unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other unfair-dealing or practice is not permitted and may lead to disciplinary action, up to and including termination.

Employees are not to engage in activities with customers, suppliers, vendors, or competitors that unfairly prevent or limit competition, or could appear to do so.

The Company is required to comply with all antitrust laws and strives to avoid conduct that may give even the appearance of being questionable under those laws. Whether termed antitrust, competition or free trade laws, the rules are designed to protect consumers and competitors against unfair business practices and preserve competition. Any activity that limits, reduces or eliminates free competition could constitute potentially unlawful anti-competitive conduct and must be avoided. The Company's policy is to compete vigorously and ethically while complying with all such rules. In all cases in which there is question or doubt about a particular activity or practice, Employees should contact management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

There is no activity that raises greater antitrust risks to the Company, or to individual Employees, than communications and dealings with competitors. Where two or more competitors coordinate with each other in ways that limit competition, the individual participants could be prosecuted and sent to jail. The Company should not enter into any agreements or understandings with competitors to:

- Fix or stabilize prices, fees, rates, commissions, or other terms and conditions;
- Fix other terms of sale or purchase;
- Restrict capacity or output;
- Refrain from supplying a product or service;
- Divide markets or customers; or
- Exclude competing firms from the market.

The Company must determine its prices unilaterally (including any pricing submissions to benchmarks or pricing matrices sent to customers), fees, spreads, commission rates, terms and conditions and other matters of actual or potential competitive significance. The Company must not share its pricing, or any other nonpublic information of competitive significance, with competitors.

Similarly, the Company must make independent decisions as to other business matters, such as the markets or lines of business in which the Company will compete, the counterparties, customers and brokers with whom we will do business, the products, platforms or technologies we will support, or the timing, size or types of transactions (or particular

transactions) in which we will participate.

Company Employees are prohibited from entering into any kind of agreement or understanding with competitors concerning prices, commission rates, terms and conditions or other matters of actual or potential competitive significance. This prohibition applies to any kind of informal agreement or "gentlemen's agreement," or other tacit or implied understanding concerning price or other matters of competitive significance. Unlawful arrangements may be inferred from circumstantial evidence. To avoid any inference of an anticompetitive arrangement, great care should be taken in any communications with competitors (whether in meetings, telephone conversations, e-mails or other electronic messages or otherwise).

Employees must never invite competitors to participate in collusive activities. Any Employee who receives such an invitation from personnel of a competitor should clearly state that it is against Company policy to participate in such activities or even to discuss such matters with competitors, and should immediately report the incident to their direct supervisors and the Stewart Legal Department. If Employees become aware, or have reason to suspect, that other industry participants are engaging in collusive activities, Employees should contact management, and aCompliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

Return to Top

**Conflicts of Interest**

Employees are expected to make or participate in business decisions and to take action in the course of their employment and service to the Company based on the best interests of the Company and not based on their personal interests or relationships, for personal gain or benefits, or to obtain favors or benefits for relatives and people with whom the Employee shares a financial or close personal relationship, or for any other person. For purposes of this Code, relatives and people with whom the Employee shares a financial or close personal relationship, includes a spouse, domestic partner, party to a civil union, others with whom an employee shares an intimate or romantic relationship, parent, child, grandchild, grandparent, sibling, first cousin, aunt, uncle, nieces, nephews, guardian, roommate, business partner, co- investor, guarantor, etc., but does not include nominal financial relationships. Parent, child and sibling include biological, adopted, step, foster, in loco parentis and in-law relationships.

As representatives of the Company, Employees must avoid acting in a manner that places their personal interests ahead of the best interests of the Company, and avoid activities or circumstance in which they may be motivated to act in a manner that is not in the best interests of the Company or that otherwise creates conflicts between their personal interests and responsibilities as Employees. Conflicts of interest arise when individuals or organizations have personal or organizational interests that may interfere with, or appear to interfere with, their independent exercise of judgment in business dealings. Employees must avoid having their decisions on behalf of the Company influenced (or even appear to be influenced) by conflicting interests. Employees must also avoid situations that might create the appearance of a conflict of interest, or the appearance of having the Employee's judgment or performance of duties, compromised whether or not it actually exists and whether or not the Employee believes he or she would be improperly influenced. Employees also must comply with all Company policies or procedures that seek to manage potential conflicts between the Company's interest and those of other stakeholders, such as customers, vendors, suppliers and counterparties.

If an Employee's personal relationships or matters create a conflict of interest, a potential conflict of interest, or the appearance of a conflict of interest, or if the Employee believes that there is a conflict of interest involving another Employee, the Company requires a full and timely disclosure of the facts and circumstances to management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

Members of the Company's Board also have an obligation to act in the best interests of the Company and not based on personal relationships or benefits. To avoid conflicts of interest, directors are required to disclose to the Chief Legal Office any personal interest they may have in a transaction involving the Company and to recuse themselves from participation in any decision in which there is a conflict or potential conflict between their personal interests and the interests of the Company.

*Relationship with Suppliers, Vendors, Customers, Competitors*

Employees shall not conduct business or exercise authority on behalf of the Company with any person, firm, corporation or organization in which they or any relatives and people with whom the Employee shares a financial or close personal relationship as set forth in this Code, has a material financial interest or material connection, including, but not limited to, a directorship, officership, family relationship, or significant borrowing relationship unless the Employee has prior written permission from a Compliance Officer based upon full and appropriate written disclosure of relevant facts and circumstances. To protect Employees and the Company from the appearance of a conflict of interest in this context, Employees must make appropriate written disclosures to a Compliance Officer at ethics@stewart.com.

Without the express written approval of the Company's Chief Legal Officer, an Employee or a family member of an employee may not own 10% or more of the stock of, or have other significant financial interests in or participate in the business of a supplier, vendor or customer of the Company, if the Employee directly or indirectly orders or receives the service/product from the supplier or vendor or provides the service/product to the customer. An Employee should not have any significant financial interest in a competitor of the Company. "Significant financial interest" shall mean ownership of more than 1% or more of the equity in a public company or a financial interest representing 5% or greater of the total assets of an Employee.

The purchase of title insurance or related services from the Company in the ordinary course of business does not constitute a conflict of interest.

Return to Top

*Interest in Other Businesses*

An Employee's participation in another business or outside employment or affiliation, including service as a director, advisor or consultant to any third party, whether or not related to the business of the Company, could interfere with the Employee's ability to devote proper time and attention to his or her employment by the Company.

Employees must avoid any direct or indirect financial relationship with other businesses that could cause divided loyalty. While employed by the Company, Employees must (1) disclose to management prior to beginning (or continuing, as applicable) any outside employment, business or consulting relationship; and (2) obtain prior written approval from a Compliance Officer before beginning (i) any business or consulting arrangement with a customer of or supplier or vendor to the Company, or (ii) any investment in a supplier or vendor or customer.

The Company may approve a request if the Company determines, in its sole and absolute discretion, that an outside engagement or activity: (A) will not, and is not likely to cause or result in (i) a violation or potential violation of any law or regulation, (ii) an actual or potential conflict of interest, or the appearance thereof, (iii) such outside engagement or activity encroaching or possibly encroaching upon the Employee's regular working hours, interfering with or impairing the performance of the Employee's regular duties, or otherwise affecting productivity, or (iv) subjecting the Company to criticism from third parties or regulators; or (B) is not otherwise inconsistent with the best interests of the Company.

The following are several but not necessarily all examples of outside engagements or activities that will not be approved under any circumstances: (i) employment or affiliations that violate laws or regulations; (ii) employment or affiliation with an individual, entity, government, or country/region that is on a sanctions list (e.g., OFAC's Specially Designated Nationals and Blocked Persons List), or is otherwise subject to a sanctions program applicable to the Company; (iii) engaging in any activity that is competitive with the Company or its existing or planned products, services or businesses, including employment by a financial services company which engages in such competitive activity; and (iv) employment or affiliation that requires activities or services to be performed during regular Company working hours (e.g., receiving phone calls, preparing reports, etc.), uses Company equipment or supplies, or involves information developed for or proprietary to the Company.

A passive financial investment in a customer of the Company that does not require active participation of the Employee is permissible provided that it does not create an actual, potential, or perceived conflict of interest.

*Business Referrals*

Occasionally, a customer may ask an Employee to recommend an external service provider such as an accountant, lawyer or real estate agent. An Employee may provide the names of several external service providers but may not recommend any particular one. An Employee may not provide any written or public endorsement or testament of any third party on the Company's behalf without approval of the Chief Compliance Officer.

## Fraud/Anti-Corruption

The Company is committed to developing procedures to minimize fraud. The Company has an Anti-Fraud Plan that is designed to work in concert with existing internal procedures to facilitate the prevention, detection, and investigation of all types of fraud including claims fraud, agent fraud, internal fraud, wire fraud and other types of fraud focused on the Company and its industry. The Company's Anti-Fraud Plan is designed to educate appropriate Employees on fraud detection, provide for the hiring or contracting of fraud investigators, report insurance fraud to appropriate law enforcement and regulatory authorities, and pursue restitution, where appropriate, for financial loss caused by insurance fraud. Employees are the best defense against fraud and the Company is committed to ensuring that Employees have the skills and knowledge to recognize and where necessary, investigate fraud.

*Anti-Money Laundering*

Money laundering can occur in a variety of ways. Put simply, money laundering is the process of concealing the origins of money obtained illegally by passing it through a sequence of banking transfers or commercial transactions that can include escrow or real estate transactions. The overall scheme of this process attempts to "clean" the money to the launderer in an indirect way.

There are a variety of International, Federal and State laws, rules and regulations that affect the Stewart family of companies relating to minimizing the risk of money laundering. Stewart adheres to all applicable anti-money laundering laws, rules, and regulations. Stewart makes every attempt to conduct its business in a manner that eliminates the risks associated with money laundering. Stewart's practices include not doing business with individuals, entities, and enterprises known to engage in illegal activities. FinCEN, the Financial Crimes and Enforcement Network of the U.S. Treasury Department has adopted certain regulations relating to the real estate industry to diminish money laundering risk. Stewart has created processes to comply with the reporting requirements of the FinCEN regulations and trains its Employees and independent agencies in how to comply with the FinCEN rules to prevent money laundering. Stewart has also established policies and processes to mitigate wire fraud, which is a key tool used by money launderers,

In addition, various United States, and other laws prohibit Stewart from doing business with persons who have been identified as being involved in various illegal activities such as drug or arms trafficking or terrorism. These laws also restrict the Company's ability to insure, pay claims to, or otherwise do business with, certain countries or businesses located in or doing business with identified countries.

Return to Top

**Government Business**

Employees should understand that special requirements might apply when dealing with any government body (including national, state, provincial, municipal, local or other similar government agencies or divisions). Direct or indirect payments to officials of any government body at any level from either the Company's or an Employee's funds in furtherance of the Company's business are prohibited. Employees shall not offer or accept kickbacks, bribes, gifts, gratuities or anything else of value with the intent of obtaining favorable treatment from any government body. A gift that is customary in the business sector may be perceived as a bribe by a government official or law enforcement. If any situation arises with respect to this policy about which an Employee has any concern or question, the Employee should promptly review the matter with the Company's Chief Legal Officer.

*Foreign Corrupt Practices Act ("FCPA")*

The FCPA is a United States federal statute that prohibits corrupt or improper payments, gifts, or opportunities to foreign officials for the purpose or with the intention of obtaining or retaining business or obtaining an improper business advantage. The FCPA also requires U.S. -companies such as the Company to keep books and records that accurately reflect transactions and dispositions of assets and to maintain a system of internal accounting controls. The Company requires full compliance with the FCPA by all of its Employees. If an Employee has any doubt regarding any payment, the Employee must contact a Compliance Officer before the payment is made.

In order to assist the Company in obtaining or retaining business, for or with, or directing business to the Company, the Company shall not, nor shall any officer, director, Employee, or agent of the Company offer, pay, promise to pay, authorize the payment of any money; or offer, give, promise to give, or authorize the presentation of giving of anything of value including, but not limited to, employment opportunities, gifts or entertainment, and charitable contributions either directly or indirectly to:

- Any foreign official (including without limitation all employees or officers of any non-US national, state, provincial or local government or its departments and agencies, any worldwide financial organization, and any state owned or state organized entities);
- Any foreign political party or official of a political party or any candidate for foreign political office; or
- Any person, while knowing or having a reasonable belief that all or a portion of such money or thing of value will be offered, given, or promised, directly or indirectly, to any foreign official, to any foreign political party or official of a political party or to any candidate for foreign political office.
- Anything of value in this context may include travel, hospitality, entertainment, political or charitable contributions, or providing jobs or internships.

Commission or fee arrangements outside of the United States shall be made only with firms or persons serving as bona fide commercial representatives, agents or consultants. Such arrangements may not be entered into with any firm in which a government official or Employee is known to have an interest unless the arrangement is permitted by applicable law and has been specifically approved by the Company's Chief Legal Officer. All commission and fee arrangements shall be

by written contract and may not be paid in cash. Any commission or fee must be reasonable and consistent with normal practice for the industry, and payment shall be of fair and equivalent value for the services to be rendered.

An Employee shall not take any action or authorize any action which involves any illegal, unethical or otherwise improper payment of money or anything else of value. If a situation arises with respect to this policy about which an Employee has any concern or question, the Employee should, before taking any action, promptly review the matter with a Compliance Officer who is a member of the Stewart Legal Department.

For Employees based outside the United States in regions that have comparable legislation to that of the FCPA, Employees must not violate any anti-corruption laws that apply to them.

Should any questions or situations arise that relate to the FCPA, promptly notify management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

Return to Top

**Honoraria**

Speaking at events, when it is determined to be in the Company's best interests and approved by management, is considered part of an Employee's normal job responsibilities. Employees should not request or negotiate a fee or receive any form of compensation from the organization that requested the presentation. Unless otherwise stated in this Code, acceptance of continuing education credits or other novelties is acceptable.

**Inventions, Books and Publications**

Employees must receive written permission from a Compliance Officer before developing, for any party other than the Company, any products, software or intellectual property that are or may be related to the Company's current or potential business.

Return to Top

**Laws, Regulations and Government Related Activities**

It is expected that each Employee will comply with all applicable federal, state, and local laws, ordinances, and regulations. Violation of governing laws and regulations is illegal and unethical and subjects the Company and possibly the Employee to significant risk in the form of fines, penalties, damaged reputation and possible criminal sanctions.

It is the responsibility of all Employees to report any instances which they believe may constitute violations of applicable laws and regulations, regardless of whether such violations have been committed by co-workers, supervisors, officers, or directors, or by vendors, contractors, consultants, customers, or any other party having a business relationship with the Company to management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

*Boycotts*

All Employees must abide by applicable United States anti-boycott laws, which prohibit United States persons, United States. Companies and their overseas branches and subsidiaries, from taking actions or entering into agreements that could aid unsanctioned foreign boycotts of certain countries. Generally speaking, anti-boycott laws prohibit actions, and

agreements to take such actions, that could further any boycott not approved by the United States, such as:

- Refusing to do business with or in a boycotted or blacklisted country or with nationals or residents of a boycotted country;
- Discriminating against other persons based on race, religion, sex, national origin, or nationality;
- Furnishing information about business relationships with or in boycotted countries or blacklisted companies;
- Furnishing information about the race, religion, sex, or national origin of another person;
- Furnishing information, about business relationships with blacklisted companies or with blacklisted persons; or
- Implementing letters of credit containing prohibited boycott terms or conditions.

Employees should refer any request that appears to be boycott-related to management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

*Office of Foreign Assets Control ("OFAC")*

OFAC administers and enforces economic and trade sanctions against countries, regimes and individuals involved in terrorism, narcotics or other illegal activities. The US economic sanctions regulations prohibit financial institutions from doing business of any kind with certain countries, groups, entities and/or individuals, with persons owned or controlled by sanctioned targets, as well as with individuals and entities that act on their behalf.

The Company and Employees may not do business of any kind with targeted governments, countries, regions and organizations, as well as individuals, groups and entities identified on the OFAC Specially Designated Nationals and Blocked Persons List/Foreign Sanctions Evaders Lists or is otherwise subject to a sanctions program applicable to the Company.

*Privacy Laws and Policies*

One of the Company's most important asset is our customers' trust. Keeping customer information secure and using it appropriately is a top priority for the Company. Employees must safeguard any confidential information our customers share with us. Employees must also ensure that they use customer information only for the reasons for which the information was gathered, unless further use is allowed by law. The Company has in place privacy principles that detail our specific commitments to customers, and processes that define, document, monitor and manage the security of information.

In addition, many countries have data protection and privacy laws that affect the collection, use and transfer of personal customer information. This is a rapidly changing area of law, and Employees should consult management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com. Employees should contact a Compliance Officer with any questions regarding appropriate uses of customer information.

Applicable law mandates that employers restrict access and the dissemination of certain personal or private information, including but not limited to Employee medical and personnel records, to only those who have a legitimate business need or use for the information. This may include third-party vendors engaged to support specific business functions. Such records must not be shared or discussed inside or outside the Company, except as authorized by the Employee; as appropriate with authorized Employees and management in the course of employment; as required to support the Employee in the administration of benefits or leave of absence with a designated vendor; or as required by law, rule, regulation, or a subpoena or order issued by a court of competent jurisdiction or requested by a judicial or administrative or legislative body with competent jurisdiction. Requests for such records from anyone outside the Company under any other circumstances must be approved by the Company's Chief Human Resource Officer or designee, with the approval of the Company's Legal Department. For Employees based outside the United States, approval for same must come from the

appropriate Head of Human Resources.

For further information, please see the Company's Privacy Policy at stewart.com. For Employees based outside the United States, refer to the Privacy Policy or Data Protection Policy relevant for the jurisdiction, as referenced in the related Schedules.

Return to Top

*Real Estate Settlement Procedures Act ("RESPA") and Consumer Financial Protection Bureau ("CFPB")*

RESPA governs our relationships with lenders, real estate professionals, buyers, sellers and other settlement service providers in most residential transactions. RESPA applies to any transaction involving a federally insured mortgage on one-to-four-unit residential property, including purchase loans, assumptions, refinances, property improvement loans, reverse mortgages and home equity lines of credit. In general, RESPA prohibits the payment of kickbacks or fees in exchange for the referral of settlement service business and requires that borrowers receive certain disclosures. Both civil and criminal penalties can result from RESPA violations. It is essential that Employees comply fully with RESPA. Prohibited Practices under RESPA include:

*Kickbacks and Referral Fees*

The Company and its Employees must not give or accept any kickback, fee, or other thing of value in exchange for referrals of settlement service business. For example, RESPA prohibits settlement service providers from giving others who refer business gift certificates, prizes (such as a chance to win a trip), or even inexpensive items in exchange for referrals. Regulators may also presume that any amount paid to a referral source in excess of fair market value for a service or product (such as renting office space from a broker or lender at above-market rates or paying a disproportionate share of joint advertising) is an illegal referral fee. In contrast, it is permissible under RESPA for a settlement service provider to give consumers a discount or a similar inducement to do business with the Company where permitted by state law.

*Unearned Fees*

The Company and its Employees must not pay fees, split fees or receive fees for services not actually performed. For example, a borrower may not be charged a fee for sending documents via courier when the borrower personally picked up the documents. Additionally, a title agency that does not perform the usual agency tasks, such as examination of title, cannot be paid its usual fee. Employees need to be certain in all cases that reasonable payments are made, and reasonable fees accepted for services actually provided in accordance with applicable law.

*Affiliated Business Arrangement Disclosures ("AfBA Disclosures")*

An AfBA Disclosure must be given any time an Employee refers a borrower to a provider of settlement services in a one-to-four-unit residential transaction if the Company or an Employee has an ownership interest of more than one percent in the provider. An AfBA Disclosure informs the borrower about the relationship between the Company (or the Employee) and the settlement service provider and also contains an estimate of the provider's settlement service charges. The disclosure must be provided in the form required by the CFPB. If the Employee makes the referral while meeting with a borrower face-to-face, the AfBA Disclosure must be given prior to or at the time of the referral. If the Employee makes the referral by telephone or electronic media, the Employee must give the AfBA Disclosure within 3 business days of making the referral. An AfBA Disclosure is not required when trying to win business for the Company. For example, if an Employee who is a closer tells a friend what good service we can provide in connection with his home purchase, an AfBA Disclosure does not need to be provided at that time. If an Employee refers a residential customer to a joint venture or other third-

party in which the Company is a part-owner, a timely AfBA Disclosure must be given.

An Employee who refers a borrower to an affiliated settlement service provider must not require the borrower to use that particular service provider. For example, an Employee may recommend, but not require, that a borrower use a lender with whom the Company has an affiliated business arrangement ("AfBA"). This prohibition is noted on the AfBA disclosure form.

Return to Top

*TILA-RESPA Integrated Mortgage Disclosures*

The CFPB requires TILA-RESPA Integrated Mortgage Disclosures. The disclosure requirements apply to all closed-end consumer mortgage loans secured by real property purchased primarily for personal, family or household purposes – including construction loans, loans on 25 acres or more of vacant land, or single-family residence loans. Evidence of compliance with the integrated mortgage disclosure rule in effect should be preserved and retained in the files of the title insurance company, direct operation, or title insurance agencies in accordance with Company policy and record retention requirements.

*State Law and RESPA*

Certain states may have stricter laws governing settlement practices and following these RESPA guidelines may not be sufficient to comply with those state laws. If an Employee has any questions regarding the proper procedures to follow, the Employee should contact management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

*Using Third-Party Copyrighted Material*

Employees may sometimes need to use third-party copyrighted material to perform their jobs. It is against Company policy and may be unlawful for any Employee to copy, reproduce, scan, digitize, broadcast or modify third-party copyrighted material in his or her work for the Company, unless written permission from the copyright holder has been obtained prior to the proposed use or unless the "fair use" doctrine is applicable. Improper use of copy-righted material could subject both the Company and the Employees involved to possible civil and criminal actions for copyright infringement. It is against Company policy for Employees to use the Company's facilities for the purpose of making or distributing copies of third-party copyrighted materials for personal use or for use by others.

Return to Top

## Political Activity

The Company does not have a Political Action Committee (“PAC”) nor does the Company use any of the Company’s funds to contribute to any political campaign. However, the Company respects the right of Employees to participate in the political process and encourages them to engage in political activities should they desire to do so. Employees may participate in any lawful political activities of their choice on an individual basis, with their own money or resources and on their own time. Employees may not use their work time in any political campaign, offer the use of the Company’s facilities, equipment, or personnel, contribute on behalf of the Company, or direct any payment or expenditure of Company funds for any political campaign contributions or purposes or in connection with any election or primary whether within the United States or internationally, unless such use has been approved in advance by the Company’s Chief Compliance Officer.

Employees who are considering becoming a candidate for elective public office must obtain prior written approval fromthe Company's Chief Compliance Officer to be certain there will be no conflict of interest or other possible violation of law. Employees who are considering acceptance of other significant political responsibilities (such as a campaign manager or campaign treasurer, or serving on a campaign staff, campaign advisory committee, campaign finance committee or political action committee) in connection with an identifiable campaign for a specific candidate or proposition, or who are considering acceptance of appointment to any governmental position, must provide notice reasonably in advance of engaging in such activities and obtain prior written approval.

While guidance and appropriate approval must be sought prior to carrying out the political activities described herein, examples of activities that may be deemed appropriate include hosting political candidates at Company offices for the purpose of informing the candidate about the Company's business, engaging in communication with legislators to further the Company business interests, and engaging in lobbying or regulatory compliance activities by Employees whose core job functions include these responsibilities. However, federal, state and local laws regulate lobbying activities, such as requiring parties that engage in lobbying activities to register as a lobbyist or lobbying entity and to make regular disclosures about their lobbying activities. Without express written authorization from the Chief Legal Officer, Employees are prohibited from engaging in any lobbying activities on behalf of the Company. Employees who fail to comply with this section may be subject to disciplinary action, up to and including termination of employment.

Return to Top

**Personal Use of Corporate Property and Corporate Information**

An Employee shall not:

- Use or divert any Company property, including the services of other Employees, for his or her own advantage or benefit or for the advantage or benefit of his or her relatives and people with whom the Employee shares a financial or close personal relationship. All Company assets should be used only for legitimate business purposes. Any personal use of Company assets must be in accordance with Company guidelines. If not needed for Company business, Company assets may be purchased at prices published by the Company;
- Take for himself or herself opportunities that are discovered through the use of Company property, information, or position or in the course of conducting Company business or which could constitute a business opportunity for the Company;
- Compete with the Company;
- Use Company letterhead paper when sending letters on personal or other matters not directly related to the Company's business, except for use of Company letterhead with prior management approval for civic and charitable causes that enhance the Company's reputation in the community; or
- Use Company email for personal use or other matters not directly related to the Company's business to promote a personal, social or political agenda, or to give the impression that personal views expressed in Company email are the views of the Company.

Return to Top

*Confidential Information*

One of the most important job duties of all Employees is the expectation that Employees will maintain their duty of loyalty to the Company. As part of an Employee's job, he or she is expected to perform all duties and assignments with the Company's legitimate business interests in mind and in the best interest of the Company. An Employee is also expected not to take any actions that would directly conflict with the Company's legitimate business interests. The protection of confidential, proprietary business information and trade secrets is vital to the interests and the success of the Company.

Confidential, proprietary and trade secret information is provided to Employees only for use in their primary job duties and responsibilities. Each Employee shall use all reasonable care to protect or otherwise prevent the unauthorized disclosure of such information. In no event shall confidential proprietary and trade secret information be disclosed or revealed within or outside the Company without proper authorization or purpose. Generally, such information should be communicated or disclosed within or outside the Company only if the recipient of the information: (i) has a legitimate need-to-know such information in connection with his or her duties and responsibilities; and (ii) has no responsibilities or duties, whether to the Company or others, that are likely to give rise to an actual or potential conflict of interest, or the appearance thereof, or a misuse of such information. When confidential information is communicated to someone, the recipient should be clearly informed that the information is confidential and be given instructions about the limitations on further dissemination of the information. Additionally, Employees may also not use cameras, cell phones, webcams or other image or sound recording devices to take images of confidential, proprietary or trade secret information or material. If an Employee is uncertain whether certain information should be treated as confidential, the employee should presume that such information is confidential and not disclose it without proper authorization.

By way of example, confidential or proprietary information will include without limitation information and data regarding Company's business strategies and methods, business plans, databases, systems and software, technology, software reports and copies of reports, intellectual property, know-how, current and future sales/marketing/promotional plans, business development, operations, products, services, research, development, inventions, financial information and statements, financial forecasts, financing methods, pricing strategies, customer sources, referral sources, employee health/medical records, system designs, customer lists and personal identifying information, customer account and transaction/proposed transaction information, customer creditworthiness information, Employee lists, methods of competing, written summaries, verbal disclosures and pictures.

The confidential relationship between the Company and each of its customers is a fundamental principle long recognized by law. For this reason, every Employee must respect and maintain the confidential nature of the business of the Company's customers, prospective customers and other parties dealing with the Company. Transactions, correspondence, conversations and negotiations involving customers or other parties dealing with the Company must never be discussed with other customers or parties, or with Employees who do not have a legitimate need to learn such information, or in any way made public. Even the fact that a person or entity is a customer of the Company or other party dealing with the Company should be treated as confidential Information. Caution in discussing customer information and/or the existence of customer relationships must be exercised in both business and social situations.

Employees may not use confidential, proprietary or trade secret information obtained in the course of employment with the Company for any personal purpose, including to further a private interest or make a personal profit. Likewise, Employees may not permit others (such as relatives and people with whom an Employee shares a financial or close personal relationship) to use any confidential, proprietary or trade secret information for any purpose.

Employees who improperly use or disclose trade secrets or other confidential, proprietary business information will be subject to disciplinary action, up to and including termination of employment and legal action, even if they do not actually benefit from the disclosed information.

Compliance with this policy requires that each Employee exercise care to reduce the likelihood of unauthorized disclosures of confidential proprietary and trade secret information. Employees must guard against even seemingly innocent or inadvertent disclosures to spouses, friends and unauthorized Employees.

Confidential or proprietary and trade secret information should be properly safeguarded at all times. No Employee should attempt to obtain such information, which does not relate to an Employee's employment duties and responsibilities.

Employees must also refrain from using any confidential information belonging to any former employers, and such information must never be introduced to the Company or its systems, used on behalf of the Company or during the course of work for the Company or provided to other Employees. Employees must treat all confidential or proprietary information and trade secrets as such both during and after their employment.

Confidential information does not include information lawfully acquired by non-management Employees about wages, hours or other terms and conditions of employment, if used by them for purposes protected by Section 7 of the National Labor Relations Act such as joining or forming a union, engaging in collective bargaining, or engaging in other concerted activity for their mutual aid or protection.

This Confidential Information section is in no way intended to limit the right of Employees to report alleged violations to governmental and regulatory authorities or provide information or otherwise assist governmental and regulatory authorities in an investigation.

Return to Top

*Insider Trading*

If an Employee becomes aware of material non-public information in the performance of his or her duties, he or she must hold that information in the strictest confidence and refrain from buying or selling (or influencing others to buy or sell) any stock or other securities of the Company until the information is public. This policy also applies to trading in the securities of any other company, including our customers or suppliers and other vendors, if Employees have material, non-public information about that company. Buying or selling securities before the information is publicly disclosed could be considered "insider trading," and could result in both civil and criminal penalties, both to the Employee personally and to the Company.

"Material non-public information" means facts that have not been disclosed to the public that could influence a reasonable investor's decision to buy or sell a company's stock or other securities. Examples of information that could be considered material non-public information (until appropriate public disclosure has been made) for these purposes includes information regarding quarterly or annual earnings, a change in the dividend, a stock split, a merger, an acquisition, disposition or consolidation or financial information that is not generally known or expected on the basis of publicly known factors.

In addition to the obligation to refrain from trading while in possession of material non-public information, Employees are also prohibited from "tipping" others regarding such information. “Tipping” is considered a form of insider trading and is a serious breach of Company confidentiality. For this reason, Employees should be careful to avoid discussing sensitive information in any place (for instance, at lunch, on public transportation or in elevators) where others may overhear such information. Any question regarding insider trading issues should be addressed to management, a Compliance Officer at ethics@stewart.com, or EthicsPoint at (866) 384-4277 or www.ethicspoint.com.

Employees must also adhere to the Company’s Securities and Trading Investment Policy.

Return to Top

**Retention of Records**

In order to meet its financial, legal, regulatory and operational objectives and requirements, it is important that the

Company maintains adequate records. Company records include paper documents (originals and photocopies), electronic mail and messages and other electronic and digital data and records. The length of time that Company records must be retained will vary depending on the type of document/information and applicable legal and other requirements. A Compliance Officer or management should be consulted regarding the requirements for record retention and destruction of Company documents.

Notwithstanding any Company records retention policy, an Employee must never destroy or relocate any document or record or information if the Employee believes that it may be applicable or relevant to any pending, threatened, or likely claim, controversy or proceeding, whether investigative, administrative regulatory or judicial.

Return to Top

## Conclusion

Compliance with the terms of this Code is a condition of employment, and continued employment with Company. Employee conduct in violation of these standards is unacceptable and will be considered in all cases to be outside the scope of the Employee's employment. An employee who has been found by the Company to have violated or engaged in conduct inconsistent with the Code and/or any Company policy is subject to disciplinary action, up to and including termination of employment and may be subject to civil and criminal action.

This Code does not constitute or establish an employment contract, and nothing in this Code changes the at-will nature of employment with the Company. Adherence to this Code is a condition of employment and continued employment with Company. Periodic requested certification is part of this requirement, and failure to do so within the required time may result in disciplinary action up to and including termination of employment.

# Stewart Code of Business Conduct and Ethics: Schedules for Areas outside the United States

## Table of Contents



## Policy

### Schedules for Areas outside the United States

The Stewart Code of Business Conduct and Ethics ("Code") has additional terms and conditions as provided below in the Schedules for specific areas outside the United States. In the event of a conflict between the Code above and the Schedule for a specific area, the Schedule shall control. For all areas, reference to "Compliance Officer" includes the Company's Chief Compliance Officer, in addition to any specific individuals referenced in each Schedule.

Return to Top

### Schedule A – Australia

This Schedule relates to and forms a part of Stewart's Code of Business Conduct and Ethics ("Code") and is applicable to Stewart Title Guaranty Company, Stewart Title Company, and applicable Stewart Family of Companies (collectively "Stewart" or the "Company"). For Australian Employees, reference to "Compliance Officer" in the Code is in reference to the General Counsel – Australia; Vice President of Human Resources – International Group; Vice President, Chief Compliance and Risk Officer – International Operations; and Associate General Counsel – International Operations.

*Privacy Policy*
Australian Employees are subject to the Privacy Policy set out at: http://stewartau.com/public/Privacy.html

*Record Retention Policy*
Australian Employees are subject to the Record Retention and Destruction Policy as set out at: http://interpoint/canada/main/Australia/Shared%20Documents/Forms/AllItems.aspx

*Fraud Management Policy*
Australian Employees must be aware of and refer to the Fraud Management Policy as set out at: http://interpoint/canada/main/Australia/Shared%20Documents/Forms/AllItems.aspx
The purpose of a fraud management policy is to promote fraud awareness, fraud detection and outline fraud response strategies and procedures in order to promote an effective risk management environment for Australian Employees.

*Risk Management Policy*
Australian Employees must be aware of and refer to the Risk Management Policy as set out at:
http://interpoint/canada/main/Australia/Shared%20Documents/Forms/AllItems.aspx
The purpose of a risk management policy is to promote awareness of Stewart Title's Risk Management Framework in order to promote an effective risk management culture among Australian Employees.

*FCPA*
Australian Employees must be aware of the requirements established in the FCPA as set forth in the Code.

Australian Employees should also be cognizant of equivalent governing legislation in Australia subsumed within Division 70 of the Criminal Code Act.

Division 70 of the Criminal Code Act provides a definition of what it considers to be the bribing of a foreign government official and the penalties that may ensue for both individuals and corporations if convicted of said crime.

In addition to being conversant with the FCPA bribery violation provisions, it is important for Australian Employees to be mindful of the fact that Division 70 of the Criminal Code Act contains similar language and applies to the Company's Australian branch as well.

Return to Top

**Schedule B – Canada**

This Schedule relates to and forms a part of Stewart's Code of Business Conduct and Ethics ("Code") and is applicable to Stewart Title Guaranty Company, Stewart Title Company, and all of their majority owned applicable Stewart Family of Companies (collectively "Stewart" or the "Company"). For Canadian Employees, reference to "Compliance Officer" in the Code is in reference to the Vice President – Legal for Canada, Vice President of Human Resources – International Group, Vice President, Chief Compliance and Risk Officer – International Operations and Associate General Counsel – International Operations.

*Privacy Policy*
Canadian Employees are subject to the Privacy Policy set out at:
English: http://www.stewart.ca/Privacy.html
French: http://www.stewart.ca/fr-CA/Privacy.html

*Record Retention and Destruction Policy*
Canadian Employees are subject to the Record Retention and Destruction Policy set out at:
http://interpoint/canada/main/Legal/POLICY%20Record%20Retention%20%20Destruction%20Policy%20Versio/Forms/AllItems.aspx

*Anti-Spam Policy*
Canadian Employees are subject to the Anti-Spam Policy set out at:
http://interpoint/canada/main/Legal/POLICY%20AntiSpam%20Policy%20Version%201/POLICY%20-%20Anti-Spam%20-%20Final%20(Oct%202015).pdf

*FCPA*
Canadian Employees must be aware of the requirements established in the FCPA as set forth in the Code.

Canadian Employees should also be cognizant of equivalent governing legislation in Canada subsumed within the Corruption of Foreign Public Officials Act.

The Corruption of Foreign Public Officials Act applies to all acts undertaken by Canadians worldwide in connection with the bribing of a foreign official; there is no real and substantial link to Canada required.

In addition to being fully conversant with the FCPA bribery violation provisions, it is important for Canadian Employees to be mindful of the fact that the Corruption of Foreign Public Officials Act contains similar language and applies to the Company's Canadian branch as well. Employees in this region need to review the Corruption of Foreign Public Officials Act on a regular basis and be familiar with same.

*Anti-Trust*

Canadian Employees are expected to comply with the following Anti-Trust provisions:

In Canada, the anti-trust statute is the federal *Competition Act* which prohibits a number of behaviors which may include, but are not limited to:

- Abuse of Dominance, where a company with market power engages in certain practices which are intended to reduce or prevent competition;
- Misleading advertising;
- Refusing to supply a product to a customer without legitimate reason which may make the customer unable to carry on his/her business;
- Price discrimination;
- Price maintenance;
- Bid-Rigging, in which competitors agree as to who to bid on a call for tenders; and
- Conspiring with competitors, in which competitors conspire or agree to fix prices, allocate customers or restrict output.

No Employee should discuss pricing, coverage, customers, or market share, or such matters directly or indirectly with competitors.

The Company fully embraces all antitrust laws and avoids conduct that may give even the appearance of being questionable under those laws. Whether termed antitrust, competition or free trade laws, the rules are designed to keep the marketplace thriving and competitive. In all cases in which there is question or doubt about a particular activity or practice, Employees should contact their manager and ethics@stewart.com regarding any questionable activity.

*Real Estate Settlement Procedures Act ("RESPA")*

For Canadian Employees, note that while RESPA is a US statute, and accordingly does not govern Canadian Employees with respect to transactions occurring in Canada with respect to Canadian properties, the principles contained therein apply to Canadian Employees and would fully govern any transactions taking place in the USA. In particular Canadian Employees should be aware of the prohibition from giving or accepting any kickback, fee or other thing of value in exchange for referrals or other advantage.

*Canada's Anti-Spam Legislation*

Canadian Employees are required to read and acknowledge the Company's policy with respect to Canada's Anti-Spam Legislation ("CASL"). CASL is designed to protect Canadians from receiving unsolicited commercial electronic messages ("CEM") (such as emails and texts). CEMs are messages that are meant to encourage commercial activity (i.e., promoting sales or use of a service).

Very specific rules are set out as to what constitutes a CEM, what consent is needed (or not) to send out a CEM, and the requirement for unsubscribe functionality. In general, the Communications Department is the only department authorized to send CEMs. Business Development representatives who have received training may also send certain CEMs. Note that CASL applies regardless of the place of origin of the CEM as long as the recipient is in Canada. Thus, using a foreign company to outsource the sending of CEMs to Canadians will not eliminate the need to comply with CASL.

Please review the Company's Anti-Spam policy for full details.

Return to Top

**Schedule C – UK and Europe**

This Schedule relates to and forms a part of Stewart's Code of Business Conduct and Ethics ("Code") and is applicable to Stewart Title Guaranty Company, Stewart Title Company, and applicable Stewart Family of Companies (collectively "Stewart" or the "Company"). For UK and European Employees, reference to "Compliance Officer" in the Code is in reference to the General Counsel for UK and Europe, Vice President of Human Resources – International Group, Vice President, Chief Compliance and Risk Officer – International Operations, Associate General Counsel – International Operations.

*Privacy Policy*
UK and European Employees are subject to the Personal Data Protection Policy set out in the Associates Handbook and at: http://www.stewarttitle.co.uk/content/dam/stewart/stewart-uk/PDFs/UK-Personal-Data-Protection-Policy_01-2014.pdf

*Foreign Corrupt Practices Act ("FCPA")*
UK and European Employees must be aware of the requirements established in the FCPA as set forth in the Code.

UK and European Employees should also be cognizant of equivalent governing legislation in the UK subsumed within the United Kingdom Bribery Act 2010.

The United Kingdom Bribery Act 2010 applies to all acts undertaken in connection with the bribing of a foreign official and provides for extra-territorial jurisdiction over UK residents, citizens and corporations located worldwide. It also imposes, amongst other things, strict liability on a business for failing to prevent "Associated Persons" from committing the bribing of a foreign public official.

In addition to being conversant with the FCPA bribery violation provisions, it is important for UK and European Employees to be mindful of the existence of the United Kingdom Bribery Act as well.

Return to Top