proofpoint

PROOFPOINT, INC.

BUSINESS CONDUCT GUIDELINES

As Adopted by the Board of Directors
on April 19, 2012[1]

1. Standards of Conduct

Proofpoint expects everyone to act with the highest standards of honesty and ethical conduct. We consider honest conduct to be conduct that is free from fraud or deception and is characterized by integrity. Proofpoint considers ethical conduct to be conduct conforming to accepted professional standards of conduct. We must comply with all laws, rules and regulations applicable to Proofpoint and its business, as well as applicable policies and procedures. Each employee, officer and director must acquire appropriate knowledge of the legal requirements relating to his or her duties sufficient to enable him or her to recognize potential problems and to know when to seek advice. Violations of laws, rules and regulations may subject the violator to individual criminal or civil liability, as well as to discipline by Proofpoint. These violations may also subject Proofpoint to civil or criminal liability or the loss of business.

2. Your Responsibilities

(a) Read Our Business Conduct Guidelines

Proofpoint is committed to the highest level of integrity and ethics in running all aspects of its business. Honesty, loyalty and accountability are core to our values and we are committed to building a culture of compliance. Our credibility, reputation and brand depend on the actions of everyone at Proofpoint—from new hires to board members. In order to align our actions with Proofpoint's values, these Business Conduct Guidelines (the "Guidelines") include information about the laws, ethics, policies and processes that apply to our company. The Guidelines apply to all employees, officers and directors and to Proofpoint affiliates and subsidiaries worldwide. Inside, you'll find both company policies and instructions regarding your obligations, including how to report an incident or get advice regarding compliance. It is your responsibility to read the Guidelines carefully. In addition, you should carefully review each policy referred to in the Guidelines. Please take the time to review the Guidelines at least once per year. Everyone at our company is responsible for understanding the Guidelines so that our behavior meets our standards.

These Guidelines are a statement of fundamental principles, policies and procedures that govern the Company's employees, officers and directors in the conduct of the Company's business. It is not intended to and does not create any legal rights for any supplier, partner, competitor, stockholder or any other person or entity.

(b) Use Common Sense and Ask Questions

While the Guidelines are intended to cover all our policies and scenarios, we understand that issues may arise that are not covered directly. We rely on your good judgment in all situations. When making a decision, always ask yourself how your choices may be portrayed in a public forum. In addition, our compliance team is always here to help answer any questions.

(c) How to Raise a Concern

[1] Modified 7/18/2015 to reflect new whistleblower hotline
Modified 10/19/2016 as part of ongoing annual review

In order to raise concerns or ask questions, please contact your supervisor or manager, your Human Resources representative or the Legal Department at ComplianceReports@proofpoint.com. If you prefer to remain anonymous, you may contact us via mail at Proofpoint, Inc., 892 Ross Drive, Sunnyvale, CA 94089, Attention: Compliance Officer or at 1-844-684-4269 or via the web at www.reportlineweb.com/proofpoint.[2] No matter how you choose to contact us, we prohibit retaliation against anyone raising a concern in good faith. We are here to help you—please contact us with any comments or questions.

3. Complying with Laws

(a) You must comply with the laws, rules and regulations in each country where we conduct business. As we are a company headquartered in the United States, these Guidelines are based primarily on U.S. laws. While local laws may in some cases be less restrictive than these Guidelines, you must comply with the Guidelines even if your conduct would otherwise be legal. In cases where local laws are more restrictive than the Guidelines, you must comply with the applicable local laws. Remember to contact the Legal Department if you have questions.

(b) Insider Trading

Insider trading, insider dealing and stock tipping are criminal offenses in most countries. The purpose of our insider trading policy is to establish guidelines to ensure that we all comply with laws prohibiting insider trading. Our Insider Trading Policy prohibits the purchase or sale of Proofpoint securities by persons who are aware of material information about Proofpoint that is not generally known or available to the public. You are also prohibited from disclosing this information (also known as "tipping") to others who may trade. Material information is any information that a reasonable investor would consider important in a decision to buy, hold, or sell securities. It includes any information that could reasonably be expected to cause a change in the price of securities of Proofpoint or the securities of another company to which the information relates. Similarly, if you become aware of material non-public information about other companies, such as Proofpoint partners, suppliers or customers, through your work at Proofpoint, you may not trade the securities of such companies.

The Insider Trading Policy also restricts certain parties who are likely to have access to material non-public information from engaging in any transactions in Proofpoint securities during quarterly blackout periods and until adequate public disclosure of the information has been made. In addition, certain parties must obtain prior written approval for all transactions of Proofpoint securities, regardless of when they occur. If you are considering a stock transaction, and you believe you may have material non-public information, consult the Insider Trading Policy and the Insider Trading Compliance Officer at TradingRequest@proofpoint.com.

Anyone who knowingly trades Proofpoint securities while in possession of material non-public information or who tips information to others will be subject to appropriate disciplinary action up to and including termination.

(c) Anti-Corruption and Anti-Bribery

No one acting on Proofpoint's behalf may, directly or through intermediaries, use bribes or other corrupt practices in conducting Proofpoint business to influence business conduct and/or any federal, state, or local government employee in any country. No matter where you are located, you must comply with all elements of the U.S. Foreign Corrupt Practices Act ("FCPA") and the Proofpoint Anti-Corruption and Anti-Bribery Policy. The FCPA prohibits giving or offering to give anything of value, any payment, gift, entertainment, or service to foreign government officials, their immediate family members, their employees, foreign political parties, candidates or public international organizations, such as the United Nations (collectively, "Government Actors"), or any third party with knowledge that that offering will be forwarded to a Government Actor for the

[2] International employees may contact the anonymous whistleblower hotline via international toll free numbers which are listed on our internal wiki on the ethics and compliance page. You may also register a concern via the Internet at https://iwf.tnwgrc.com/proofpoint.

purpose of obtaining or retaining business or to secure an improper advantage. If you engage in any of the foregoing, you may expose both yourself and Proofpoint to civil and criminal penalties.

The FCPA requires the maintenance of accurate books of account, with all company transactions being properly recorded. In addition, please note that even nominal gifts pursuant to local custom to a Governmental Actor where the gift is designed to obtain or retain business or to secure an improper advantage is improper. If you believe that your work with a Governmental Actor requires certain necessary courtesies, please contact the Legal Department to ascertain the correct engagement procedures.

(d) Export and International Trade

As a technology company with worldwide operations, Proofpoint must comply with all applicable import and export control laws and trade regulations. United States trade regulations apply to many activities involving non-U.S. citizens, including doing business with such parties, transmission or shipment of software, or technical data. Some of the strictest export controls are maintained by the United States against countries that the U.S. government considers unfriendly or as supporting international terrorism. The United States and other countries restrict the export of goods, software and technology, such as some types of electronics, and encryption technology, which could have military or other applications and pose a danger to the interests of the country restricting the export. Additionally, the U.S. government restricts exports of nearly all goods and technology to, or conducting business with, certain countries. Even presenting data to a foreign national in the United States may constitute an export. The Company requires compliance with laws and regulations governing export controls in both the United States and in the countries where the Company conducts its business. Certain regulations also prohibit U.S. companies from taking any action that has the effect of furthering any unsanctioned boycott of a country friendly to the U.S. The U.S. regulations are complex and apply both to exports from the United States and to exports of products from other countries when those products contain U.S.-origin components or technology. Any questions about export control laws and regulations should be directed to Proofpoint's Chief Financial Officer or General Counsel. It is your responsibility to review and understand our Trade Compliance Policy and to consult with the General Counsel to determine whether your activities are subject to special controls, and if so, to comply with them.

4. Your Employment Relationship

Your employment relationship with Proofpoint is addressed in more depth in your employee handbook. Please consult your employee handbook for additional information.

(a) Fair Employment Practices

Proofpoint is committed to the highest standards of fairness in all its employment practices. We do not tolerate unlawful discrimination and harassment under any circumstances. Not only is this behavior illegal, it is also against Proofpoint's values. Engaging in such conduct would deteriorate the collaborative nature of our workplace, and could expose you and Proofpoint to liability. Proofpoint values the strength and ingenuity that result from a diverse workplace. It is important that we all embrace each other's differences and treat one another with respect.

(b) Diversity

Proofpoint affords equal employment opportunity to all qualified persons without regards to any impermissible criterion or circumstance. The means equal opportunity in regard to each individual's terms and conditions of employment and in regard to any other matter that affects each person's working environment. In addition, this means that every employee is protected from retaliation if the employee makes a good-faith complaint of unlawful discrimination or harassment or participates in an investigation of such employment practices.

(c) Workplace Rules

Proofpoint believes that we should all work in a safe environment. We provide training and guidelines regarding how to use your equipment and our facilities. It is important that you follow the guidelines and report anything that seems unsafe.

The safety of our workplace also depends on your behavior. Drugs and alcohol impede your ability to perform your duties and Proofpoint will take any necessary action in the case of drug or alcohol abuse. In addition, we do not tolerate workplace violence, including actions and words that may threaten another person. Violence may include words as well as actions, so you should be mindful of your behavior.

If you suspect drug or alcohol abuse, you must report it to your supervisor or manager, your Human Resources representative or the Legal Department.

5. Protecting Our Assets

(a) Using Company Resources

Proofpoint strives to furnish everyone with the assets necessary to efficiently and effectively conduct company business, including computers, communications systems, access to data and other equipment and materials. To protect Proofpoint, you should take all reasonable steps to protect against loss, theft or misuse of any of these assets. Theft, carelessness and waste have a direct impact on Proofpoint's profitability. Employees must care for equipment and use it responsibly and only for business purposes. If employees use Proofpoint equipment at their home or off site, precautions must be taken to protect such equipment from theft or damage. Employees must immediately return all equipment when their employment relationship with Proofpoint ends. While computers and other electronic devices are made accessible to employees to assist them to perform their jobs and to promote our interests, all such computers and electronic devices, whether used entirely or partially on Proofpoint's premises or with the aid of Proofpoint equipment or resources, must remain fully accessible to Proofpoint and will remain the sole and exclusive property of Proofpoint.

Proofpoint's IT systems, including the email system and the email archive, are property of Proofpoint. These assets are provided to you to conduct Proofpoint business or for purposes authorized by management. You may not use any Proofpoint asset in violation of the law or Proofpoint policies. While Proofpoint is committed to protecting your legitimate privacy interests, Proofpoint reserves the right to monitor use of Proofpoint assets in accordance with applicable laws and as necessary to protect its interests as well as store and access any emails stored in the email system or the email archive in perpetuity. If you believe that you have any personal, non-business related data that you would like to keep private, you should not use Proofpoint assets, including your Proofpoint email address, the corporate email system or the corporate network or any corporate assets or devices (such as a cell phone, tablet computer, etc.) to access, store, manage or process any such personal, non-business related data. Misuse of Proofpoint assets is misconduct and may lead to disciplinary action, including immediate termination of employment.

(b) Our Intellectual Property & Confidential Information

Non-public Proofpoint information is a vital company asset. You have a duty to maintain the confidentiality of Proofpoint information both during your employment with Proofpoint and thereafter. Proofpoint confidential information includes a wide range of non-public information including but not limited to financial analyses planning, forecasts and budgets, business and marketing plans, technology and technical information, product designs, roadmaps, and business processes. All such information must be returned to Proofpoint upon termination of your relationship with Proofpoint. Additional details about your obligations with respect to Proofpoint information are found in the agreements that you signed upon joining and that you must re-confirm upon leaving Proofpoint.

Additionally, steps must be taken to prevent inadvertent disclosure of Proofpoint confidential or proprietary information, including but not limited to discussing such proprietary or confidential information with outsiders, as well as family and friends, and in any public place, such as an elevator, restaurant or airplane. Even within Proofpoint, such information should be shared with others only on a "need to know" basis. Express authorization should be obtained before posting any proprietary or confidential Proofpoint information on forums such as Facebook, Twitter, LinkedIn, or other social media, or other web-based forums. While away from Proofpoint facilities you must take special care to protect Proofpoint's information, in both hard copy and

electronic form.

Any improper downloading or other prohibited use or disclosure of such Proofpoint information is unacceptable and may be deemed a misappropriation of Proofpoint trade secrets and proprietary confidential information. Proofpoint will take legal action in any case where it suspects any prohibited activities with its non-public Proofpoint information.

(c) Reporting Our Financial Results

All of Proofpoint's books, records, accounts and financial statements must be complete, accurate and reliable in all material respects. They must be maintained in reasonable detail, must appropriately reflect the transactions and matters to which they relate and must conform both to applicable legal requirements and to Proofpoint's system of internal controls. The making of false or misleading records or documentation is strictly prohibited. Funds, payments, receipts or assets must be recorded in accordance with our business practices and system of internal controls. Violations of laws associated with accounting and financial reporting can result in fines, penalties, and even imprisonment.

Proofpoint is required to adhere to strict accounting principles and standards of reporting. The information in Proofpoint's public communications, including filings with the Securities and Exchange Commission, must be full, fair, accurate, timely and understandable. Accurate and reliable financial and business records are of critical importance in meeting Proofpoint's financial, legal, and business obligations. If an employee has responsibility for or any involvement in these areas, they must understand and adhere to these rules. For example, anyone working in a sales function must provide truthful, accurate and complete disclosure confirmation and appropriate documentation as part of the paperwork relating to sales transactions.

Audits are instrumental to the ability of our company to identify and correct any concerns. Everyone must fully support the audit process and not take any action to fraudulently influence any public accountant or auditor performing an audit or review of Proofpoint's financial statements or business records.

If you become aware of any action related to accounting or financial reporting that you believe may be improper, you must report it immediately. Please see Section 8(c) "Additional Guidance and Reporting."

(d) Protecting Data

Proofpoint's customers, channel partners, suppliers and other business partners rely on our ability to treat their information and data responsibly and legally. You must take precautions to prevent unauthorized disclosure of confidential information. You must comply with any applicable data privacy and protection laws and Proofpoint's internal privacy, security and data-handling policies. You should not discuss sensitive matters or confidential information in public places, and they should avoid discussing confidential information on cellular phones to the extent practicable. You may not discuss the Company's business in any Internet chat room, blog, social media site or other online forum, regardless of whether they use their own name or a pseudonym, or otherwise post the Company's information on the Internet. When accessing Company emails and voicemails from personal computers and mobile devices, you should take steps to ensure that third parties are unable to access or hear information regarding the Company. Acceptance of confidential information from others must also be handled with care and in compliance with Proofpoint policies. Although Proofpoint sometimes has a business need to receive confidential information from a company or individual outside Proofpoint, you should be cautious when anyone wishes to share information based on an expectation that Proofpoint will hold it in confidence. If you become aware of any instance of inappropriate handling of information or data or any security breach, please report it immediately. Consult the Legal Department for the appropriate documentation and process for the receipt or sharing of data and confidential information with other parties. All Company emails, voicemails and other communications are presumed confidential and should not be forwarded or otherwise disseminated outside of the Company, except where required for legitimate business purposes.

(e) Lawsuits and Legal Proceedings

Proofpoint complies with all laws and regulations regarding the preservation of records. Records should be retained or destroyed only in accordance with Proofpoint's document retention policies.

Lawsuits, legal proceedings, and investigations concerning Proofpoint must be handled promptly and properly in order to protect and defend Proofpoint. You must contact the Legal Department immediately if you receive a court order or a court issued document, or notice of a threatened lawsuit, legal proceeding, or investigation. A legal hold suspends all document destruction procedures in order to preserve appropriate records under special circumstances, such as litigation or government investigations. When there is a "legal hold" in place, you may not alter, destroy, or discard documents relevant to the lawsuit, legal proceeding or investigation, regardless of Proofpoint's document retention policies. Proofpoint's General Counsel determines and identifies what types of records or documents are required to be placed under a legal hold and will notify employees if a legal hold is placed on records for which they are responsible. If you are involved on Proofpoint's behalf in a lawsuit or other legal dispute, you must avoid discussing it with anyone inside or outside of Proofpoint without prior approval of the Legal Department. You and your managers are required to cooperate fully with the Legal Department in the course of any lawsuit, legal proceeding, or investigation.

6. Avoiding Conflicts of Interest

(a) Identifying Conflicts of Interest

A "conflict of interest" occurs when a person's private interest (or the interest of a member of his or her family) interferes in any way – or even appears to interfere – with the interests of Proofpoint as a whole. When working for Proofpoint, your decisions must be based on sound judgment, not personal interest or gain. We must all consider whether our activities and associations with other individuals or companies may result in the appearance of or the existence of a conflict of interest. Conflicts of interest also arise when an employee or director (or a member of his or her family) receives improper personal benefits as a result of his or her position in the Company. In general, you should avoid any activity or association that creates, or appears to create, a conflict between Proofpoint's interests or your interests, or that might impair, or appears to impair, your ability to perform your work objectively and effectively. Here is a sample of potential conflicts of interest:

- Representing Proofpoint in any transaction in which you or a related person have a substantial interest
- Favoring a supplier or selecting a supplier for reasons other than price, quality, performance and suitability of the product or service
- Owning a substantial amount of securities in any competing business or any organization that does business with Proofpoint
- Serving as a director, manager, consultant, employee or independent contractor for any organization that does business with Proofpoint, or is a competitor (except with the specific prior knowledge and written consent of the Legal Department)
- Directly or indirectly competing with Proofpoint in buying or selling property, property rights or other interests
- Disclosing or using confidential or non-public information about Proofpoint
- Accepting or receiving gifts of any value or favors, compensation, loans, excessive entertainment or similar activities from any individual or organization that does business or wants to do business with, or is a competitor of, Proofpoint
- Participating in any business or investment opportunity known by virtue of your employment at Proofpoint
- Associating Proofpoint with, or indicating Proofpoint support for, any civic, religious, political or professional association without written approval from the Legal Department

Conflicts of interest are prohibited as a matter of Proofpoint policy. Conflicts of interest may not always be clear, so if a question arises, higher levels of management or Proofpoint's Audit Committee may be consulted. Anyone who becomes aware of a conflict or a potential conflict should bring it to the attention of a supervisor or manager, Human Resources or the Legal Department immediately.

(b) Outside Activities

In addition to the activities set forth above, certain types of activities create a heightened potential for conflicts of interest. An employee may not serve as a director, partner, employee of or consultant to, or otherwise work for or receive compensation for personal services from, any affiliate, customer, partner, supplier, distributor, reseller, licensee or competitor of Proofpoint or any other business entity that does or seeks to do business with Proofpoint. In certain exceptional circumstances, an executive officer may be permitted to serve as a director of such an entity (but in no circumstances will anyone be permitted to serve as a director of a competitor of Proofpoint). Serving in such a capacity for a company that is not an affiliate, customer, partner, supplier, distributor, reseller, licensee or competitor of Proofpoint may be permitted, but such activities must be approved in advance by the employee's supervisor or manager, Human Resources and the General Counsel.

(c) Corporate Opportunities

Employees and directors may not compete with Proofpoint or take personal advantage of business opportunities that Proofpoint might want to pursue without the prior approval of the Compliance Officer or the Board, as appropriate. Employees and directors are prohibited from taking for themselves personally (or for the benefit of friends or family members) opportunities that are discovered through the use of Proofpoint assets, property, information or position. Additionally, employees and directors may not use Proofpoint assets, property, information or position for personal gain (including gain of friends or family members) and may not compete with Proofpoint.

Employees and directors who are interested in the use of Proofpoint's property or information, or in pursuing an opportunity that they discovered through their position at Proofpoint, should consult with the Compliance Officer to determine an appropriate course of action. Even opportunities that are acquired through independent sources may be questionable if they are related to Proofpoint's existing or proposed lines of business. Employees and directors owe a duty to Proofpoint to advance its legitimate business interests when opportunities arise.

Business Gifts and Entertainment

Proofpoint believes that no gift, favor or entertainment should be accepted or provided if it will obligate, or appear to obligate, the recipient (whether a Proofpoint employee, a supplier or a partner). Any gifts and entertainment given or received must be in compliance with the FCPA and Proofpoint's Gift and Entertainment Policy and Proofpoint's Anti-Corruption and Anti-Bribery Policy. In addition, everyone must use good judgment, discretion, and moderation when giving or accepting gifts or entertainment in business settings. The giving or accepting of bribes, inappropriate, lavish or repeated gifts or other benefits is always prohibited, even if acceptable by local custom. Similarly, requesting or soliciting gifts or services, or requesting contributions from vendors, suppliers or other business partners for yourself or for Proofpoint, is prohibited in all cases. In general, providing normal sales promotion items, occasional meals or other non-cash items of minimal value is permitted. Please consult the Legal Department with any questions about what items may be considered to be of minimal value or permissible in a given situation.

Disclosing Conflicts of Interest

Your responsibility is to use your best judgment to evaluate objectively whether your outside activity, financial interest, or receipt of business gifts and entertainment may lead to divided loyalties. You must promptly disclose in writing to your supervisor or manager, your Human Resources representative, or the Legal Department any situation that could present a conflict of interest with your role at Proofpoint.

7. Working with Third Parties

(a) Our Channel Partners

Proofpoint resellers, distributors, and other channel partners are important to Proofpoint's

business and sales growth. If you work with Proofpoint channel partners, you have a duty to manage channel programs in compliance with local laws and Proofpoint's channel guidelines. If Proofpoint is also a competitor of a channel partner, some otherwise permitted activities may be restricted by law as more fully described below. There are legal limitations on the influence that Proofpoint may exert over channel partners, especially with respect to the pricing of Proofpoint's products. You are required to comply with the law and Proofpoint policies when developing and implementing Proofpoint channel pricing and promotional programs.

(b) Government Entities

When Proofpoint works with any government entity (including any state-owned enterprise or public international organization), on a country, state, or local level, Proofpoint must abide by all applicable laws, rules and regulations. Proofpoint strictly observes the laws, rules, and regulations that govern our transactions with any governmental entity. Activities that may be appropriate when dealing with nongovernment customers may be improper and even illegal when dealing with government entities.

Proofpoint policy prohibits us from providing or paying for, either directly or indirectly, any meal, travel, entertainment, lodging or gift intended for a government employee or foreign government official without consultation with and express written approval from the Legal Department. Gifts, meals, and entertainment provided by any Proofpoint employee located anywhere in the world to foreign government officials, their employees, political parties, state-owned enterprises and public international organizations are governed by the FCPA and Proofpoint's Gift and Entertainment Policy and Proofpoint's Anti-Corruption and Anti-Bribery Policy. The penalties of failing to adhere to these laws are severe and include substantial civil and criminal fines and imprisonment.

The foregoing does not apply to lawful personal political contributions. It is Proofpoint's policy to comply fully with all local, state, federal, foreign and other applicable laws, rules and regulations regarding political contributions. Proofpoint's funds or assets must not be used for, or be contributed to, political campaigns or political practices under any circumstances without the prior written approval of Proofpoint's Chief Executive Officer and, if required, Proofpoint's Board of Directors.

(c) Dealing with Competitors

Proofpoint believes in free and open competition. Competition laws regulate our relationships with our distributors, resellers, vendors and customers, as well as relationships with our competitors. You may not make agreements, expressly or implied, with any Proofpoint competitor to set pricing, production output, divide markets or customers, share pricing information or other competitive marketing information, boycott particular suppliers, customers or competitors, or to otherwise restrict the freedom of anyone to compete. In addition, attempts to discriminate in prices or terms of sale among our customers, or to otherwise restrict the freedom of anyone to compete, may be illegal. When a customer has a firm order in place with a competitor, you may not interfere with the performance of that contract.

You are likely to meet, talk to, or attend functions with individuals who work for our competitors. Even where the interaction seems innocent, be cautious about what is said, being careful to not discuss any subjects that are prohibited.

You should not attempt to obtain a competitor's confidential information, and you may not seek to obtain any information about Proofpoint competitors or other third parties illegally or in a way that involves a breach of integrity or breach of any confidentiality or employment agreement. No employee or director may take unfair advantage of anyone through manipulation, concealment, abuse or privileged information, misrepresentation of facts or any other unfair dealing practice. If you make any statements about competitors, your statements should not be false or misleading and any statements about competitors need to be fair, factual, complete, and capable of being substantiated.

(d) Engaging Suppliers

Proofpoint's suppliers make significant contributions to our success. To create an environment

where suppliers have an incentive to work with us, suppliers must be confident that they will be treated lawfully and in an ethical manner. It is our policy to purchase supplies based on need, quality, service, price and terms and conditions and to select significant suppliers or enter into significant supplier agreements though a competitive bid process where possible (and not on the receipt of special favors). In selecting suppliers, Proofpoint does not discriminate on the basis of any legally impermissible standard and most Proofpoint suppliers are generally free to sell products or services to any other party, including competitors.

(e) Communicating with the Public

In our business, we are likely to meet, talk to, or attend functions with individuals who work for Proofpoint's competitors, partners, suppliers or customers. Even where the interaction seems innocent, be cautious about what is said, being careful to not discuss anything relating to confidential information. Proofpoint has established specific policies regarding who may communicate information to the public, the press and the financial analyst communities. Below is a list of contacts for particular types of requests:

Type of Request	**Designated Contact**
Requests from securities analysts or investors	Investor Relations at: http://investors.proofpoint.com/contactus.cfm
Requests from reporters and news media	Corporate Communications at: http://www.proofpoint.com/about-us/media-contacts.php
Requests for information from governmental authorities or outside attorneys, other requests of a legal nature or request of any kind of audit	Legal Department at: Proofpoint, Inc. 892 Ross Drive Sunnyvale, CA 94089 ATTN: General Counsel
Requests for personnel references or employment verifications, salary verifications or other requests about current or former employees	Human Resources by facsimile at 408-850-4099

These designees are the only people who may communicate externally on behalf of Proofpoint. Everyone should refer all inquiries or calls from the press, from shareholders or from financial analysts to the investor relations department, who will see that the inquiry is directed to the appropriate authority within Proofpoint. No one may publish or make public statements outside the scope of employment with or service to Proofpoint that might be perceived or construed as attributable to Proofpoint without preapproval from the General Counsel. If approved, any such statement must include Proofpoint's standard disclaimer that the publication or statement represents the views of the specific author and not of Proofpoint.

8. Conclusion

(a) The Importance of Complying with the Business Conduct Guidelines

No guideline can replace the thoughtful behavior of an ethical person or provide definitive answers to all questions. Since Proofpoint cannot anticipate every potential situation, certain policies and procedures have been put in place to help us all approach questions or problems as they arise.

(b) Our Compliance Officer

Proofpoint's General Counsel has been designated as our Compliance Officer with responsibility for overseeing and monitoring compliance with these Guidelines. The Compliance Officer reports directly to the Chief Executive Officer with respect to these matters and also will make periodic reports to the Audit Committee of the Board of Directors regarding the implementation and effectiveness of these Guidelines as well as the policies and procedures put in place to ensure compliance with the Guidelines.

(c) Additional Guidance and Reporting

You can find the policies we refer to in these Guidelines on the Proofpoint intranet or by sending a request to ComplianceOfficer@proofpoint.com. Everyone is encouraged to seek guidance from supervisors, managers or other appropriate personnel when in doubt about the best course of action to take in a particular situation. In most instances, questions regarding the Guidelines should be brought to the attention of your supervisor or manager, your Human Resources representative or the Legal Department at ComplianceOfficer@proofpoint.com. If you know of or suspect a violation of the Guidelines, or of applicable laws and regulations, you must report it immediately.

If the report relates to accounting, internal accounting control over financial reporting, or auditing matters, governmental anti-bribery, banking or financial crime, you may contact us by letter addressed to the Proofpoint's corporate headquarters at 892 Ross Drive, Sunnyvale, CA 94089, marked "Attention: Compliance Officer" or by e-mail to ComplianceReports@proofpoint.com or any other means provided for under the Proofpoint Whistleblower and Complaint Policy. If you choose to report and wish to remain anonymous, please take appropriate steps to ensure your anonymity is maintained.

If the situation warrants or requires it, the reporting person's identity will be kept anonymous to the extent legally permitted and practical. Reprisal, threats, retribution or retaliation against any person who has in good faith reported a violation or suspected violation of law, these Guidelines or other Proofpoint policies, or against any person who is assisting in any investigation or process with respect to such a violation, is prohibited. Any employees involved in retaliation will be subject to serious disciplinary action by Proofpoint. Furthermore, Proofpoint could be subject to criminal or civil actions for acts of retaliation against employees who "blow the whistle" on U.S. federal securities law violations and other federal offenses. Conversely, no one may submit bad faith reports, that is, reports the person knows to be false. Any abuse, such as raising a malicious allegation, or one the person knows to be unfounded, will be dealt with as a disciplinary matter and/or an unlawful action, consistent with applicable law.

(d) Changes and Waivers

The Guidelines may be amended or modified from time to time in response to employee feedback or changes in applicable laws. While the Legal Department has the authority to interpret and make administrative changes to the Guidelines, only the Board of Directors or a committee of the Board of Directors can approve substantive changes to the Guidelines. These Guidelines supersede and replace all prior Guidelines. The most up-do-date version of the Guidelines is posted on our website. It is everyone's responsibility to periodically review the Guidelines on the website.

Waivers with respect to employees may be made only by the Chief Executive Officer, Chief Financial Officer or General Counsel, as applicable. In addition, in the case of matters involving financial reporting or accounting treatment or activities with respect to a supplier, customer, partner, or auditor, any wavier may only be made by the Chief Financial Officer. Any waiver of the Guidelines for a director, executive officer or any financial or accounting officer at the level of the principal accounting officer or controller or above, may be made only by the Board of Directors, and must be promptly disclosed if and as required by applicable law or regulation. Any waiver of the Guidelines with respect to a conflict of interest transaction required to be disclosed pursuant to Item 404 of Regulation S-K promulgated under the Securities Act of 1933, as amended, must be approved in advance by the Audit Committee.