



Code of Conduct and Ethics

Effective June 2021

Version 1.3

This document contains proprietary and confidential information of Payoneer Global Inc. and may not be disclosed or duplicated without the express written consent of Payoneer. Payoneer reserves the right to change this document at any time.

Payoneer Code of Conduct and Ethics

1. Introduction

We Are Accountable

At Payoneer, we believe acting ethically and responsibly is not only the right thing to do, but also the right way to do business. Every day as part of our work, we interact with a variety of individuals and entities—including our customers, competitors, co-workers, shareholders, vendors and government and regulatory agencies. We are committed to ensuring that our interactions with this wide audience are carried out in a respectful, business-ethical manner and in compliance with all applicable laws and regulatory requirements.

This Code of Conduct and Ethics (“Code”) applies to all officers, employees, contractors, consultants and temporary staff of Payoneer Global Inc. and its subsidiaries and affiliates (“Payoneer” or the “Company”), as well as members of the Payoneer board of directors when they act in their capacity as directors, known collectively in the Code as “employees,” and covers a wide range of business practices and standards. While it does not cover every issue that may arise, it sets out basic guidelines for how we conduct our business. All of our Payoneer directors and staff must conduct themselves accordingly and seek to avoid even the appearance of improper behavior. The Code should also be provided to and followed by Payoneer’s agents, contractors and representatives.

If a law conflicts with a policy in this Code, you must comply with the law; however, if a local custom conflicts with this Code, you must comply with the Code. If you have any questions about these conflicts, you should ask your manager how to handle the situation. In addition, we maintain more detailed policies and procedures for many of the topics covered by this Code, which are available at on [Payoneer Connect](#). Employees are responsible for knowing and abiding by these more detailed policies and procedures. When faced with questions beyond those addressed in the Code, employees are expected to follow both the spirit and letter of the Code and company policies that govern the issue.

Abiding by the standards and procedures outlined in the Code and Payoneer’s related policies is a condition of continued employment with the company. Our Code is not a contract of employment, and it does not convey any specific employment rights or guarantee employment for any specific period of time.

Those who violate the standards in this Code will be subject to disciplinary action, up to and including termination of employment. If you are in a situation which you believe may violate or lead to a violation of this Code, follow the guidelines described in Section 22 of this Code. Even well-intentioned actions that violate the law or this Code may result in negative consequences for the Company and for the individuals involved.

Throughout this Code, employees are encouraged to consult with any attorney in the Legal Department. Note that all communications with attorneys in the Legal Department or with outside counsel retained by the company that are made for the purpose of providing or receiving legal

advice are considered privileged communications. In addition, employees should be aware that the Company's attorneys are obligated to act in the best interests of Payoneer and do not act as personal representatives or lawyers for employees.

If you have any questions about the Code or any suspected improper conduct, you have a responsibility as an employee acting in the best interest of the Company to promptly raise the issue with your manager, the Chief Legal and Regulatory Officer, or any other attorney in the Legal Department, the Chief Compliance Officer, the Vice President of Internal Audit or the Chairman of the Audit Committee of the Board of Directors.

If you are a Payoneer manager, you have the increased responsibility of leading by example. We expect managers to serve as positive role models and inspire others to embrace our Code by:

- Modeling appropriate and actively practicing ethical behavior;
- Openly discussing and emphasizing the importance of business ethics and integrity;
- Maintaining and fostering a workplace environment that encourages candid discussions about ethical issues;
- Never justifying lapses in integrity because they help "the bottom line";
- Ensuring that retaliation for speaking up will not be tolerated; and
- Seeking help in resolving and escalating issues when they arise.

We Are Responsible to Speak Up

At Payoneer, we believe that all employees should feel empowered and responsible to speak up, particularly with respect to ethical concerns. You must promptly report suspected and actual violations of this Code, company policy and the law. In addition, Payoneer supervisors must deal with reports of misconduct promptly and properly. Payoneer will investigate all reported instances of questionable or unethical behavior. Investigations will be treated confidentially to the extent reasonable and possible under the circumstances. All Payoneer staff are expected to report any illegal or unethical behavior and cooperate in internal investigations.

In considering whether you believe a violation of the Code has occurred or is about to occur, you should first ask yourself:

- Could this conduct be viewed as dishonest, unethical or unlawful?
- Could this conduct hurt Payoneer? Could it cause Payoneer to lose credibility with its customers, business providers or investors?
- Could this conduct hurt other people, such as other employees, investors or customers?

If the answer to any of these questions is "yes" or even "maybe," you have identified a potential issue that you must report. By stepping forward and raising concerns, we are protecting Payoneer and each other, and doing the right thing.

We Do Not Retaliate

Retaliation is strictly prohibited against anyone who raises questions, speaks up, provides information or otherwise assists in an investigation or proceeding regarding any conduct that the

individual believes in good faith constitutes a violation of applicable laws or regulations, this Code, or Payoneer's related policies. In contrast, any employee who submits a report that he or she knows to be false, or who fails to cooperate fully in an investigation of a suspected violation, has violated this Code and shall be subject to disciplinary action.

Payoneer does not tolerate retaliation against anyone who reports, in good faith, any observed or suspected illegal or unethical behavior, including but not limited to: actual or potential ethical violations, incidents of misconduct, or any violation or potential violation of Payoneer's Code of Conduct and Ethics, suspicions of money laundering or terrorist financing, or accounting standards or controls.

Reports of retaliation or attempted retaliation should be made to the Chairman of the Audit Committee, the Chief Legal and Regulatory Officer, the Chief Compliance Officer or the Vice President of Internal Audit.

Additionally, Payoneer has established Whistleblower Procedures for the receipt, retention and treatment of complaints by employees and others. Any Payoneer officer, director or employee who receives a report of the type described in the Whistleblower Procedures is required immediately to inform the Chairman of the Audit Committee, the Chief Legal and Regulatory Officer, the Chief Compliance Officer or the Vice President of Internal Audit. The Whistleblower Procedures are attached as Exhibit A to this Code.

2. Compliance with Laws, Rules and Regulations

Obeying the law, both in letter and in spirit, is a fundamental obligation we must respect in all of our activities. No employee shall commit an illegal or unethical act, or instruct others to do so, for any reason. All employees must obey the laws of the cities, states and countries in which we operate. Although not all employees are expected to know the details of all these laws, it is important that you have a working knowledge of the relevant laws and regulations that apply to your responsibilities and know when to seek advice from managers or other appropriate personnel.

3. Anti-Bribery

Payoneer values integrity and transparency and has zero tolerance for corrupt activities of any kind, whether committed by employees or by third parties acting for and on behalf of Payoneer. It is strictly prohibited to make illegal payments or offers to private parties or government officials of any country, or to make payments to third parties where there is a likelihood that the third party will use any of the funds to make a prohibited payment. Payoneer cannot do or attempt to do, through a third party intermediary, any act that Payoneer itself is not permitted to do. Payoneer and its employees can be held liable for the actions of subcontractors, partners, agents, consultants and others acting on behalf of Payoneer.

The U.S. Foreign Corrupt Practices Act ("FCPA") and similar laws in other countries that apply to Payoneer prohibit promising, authorizing or giving anything of value, directly or indirectly, to a non-U.S. government official to influence the misuse of the official's position or secure an improper advantage in an effort to win or retain business. A non-U.S. government official is defined broadly and can be any official or employee of any non-U.S. government department, agency or state-

owned company; officers or employees of public international organizations (such as the United Nations); any non-U.S. party officials or political candidates. Making a facilitation payment to a non-U.S. government official to perform a non-discretionary function that is part of his or her assigned duties is prohibited under the laws of the countries in which we operate and so such payments are not permitted. Bribery involving private parties can also be prosecuted under other U.S. federal and state laws. Also, other international anti-corruption laws, such as the UK Bribery Act and the Irish Criminal Justice (Corruption Offences) Act 2018, make it a crime to offer or pay bribes or kickbacks to private parties as well as government officials.

In addition, the U.S. government has a number of laws and regulations regarding business gratuities which may be accepted by U.S. government personnel. The promise, offer or delivery of a gift, favor or other gratuity to an official or employee of the U.S. government in violation of these rules would not only violate Payoneer policy but could also be a criminal offense. State and local governments, as well as non-U.S. governments, may have similar rules. Legal and Compliance can provide guidance to you in this area.

To help ensure compliance with anti-corruption laws, all business transactions must be properly authorized, and must be completely and accurately recorded on Payoneer's books, records and accounts. You are expressly forbidden from making false or misleading entries in Payoneer's books, including entries that fail to reflect improper transactions (e.g., kickbacks and bribes) and/or entries that are falsified to disguise improper transactions. Additionally, no secret or unrecorded fund or asset of Payoneer shall be created or maintained.

If you have any questions or concerns, please always consult with the Chief Legal and Regulatory Officer, or any attorney in the Legal Department, the Chief Compliance Officer or the Vice President of Internal Audit. For more information, employees should review the Company's Anti-Corruption Policy.

4. Anti-Fraud

Payoneer is committed to detecting, preventing and addressing potential or actual fraud. Any activity you reasonably believe or suspect constitutes fraudulent activity, including fraudulent financial reporting, misappropriation of assets, bribery, forgery, extortion, theft, conspiracy, collusion, embezzlement or corruption involving an employee, or clients should be immediately reported as described in Sections 22 and 24 of this Code. An individual may also contact the Chief Financial Officer to report the potential fraud event. Payoneer's Audit Committee will oversee treatment of concerns regarding accounting, internal accounting controls and auditing matters.

5. Anti-Money Laundering, Anti-Terrorist Financing and Sanctions

Payoneer is committed to conducting business only with reputable clients and third parties engaged in legitimate business activities with funds derived from legitimate sources. Payoneer has obligations under a variety of anti-money laundering laws in many countries, including, in the United States, the Bank Secrecy Act and the USA PATRIOT Act. Payoneer takes seriously its obligations to join with governments, international organizations, and other members of the financial services industry to help close off the channels of money laundering. We have implemented applicable policies with the aim of reasonably preventing the use of Payoneer

systems, products and services for money laundering or terrorist financing activities.

Money laundering is knowingly engaging in a financial transaction with the proceeds of criminal activity in order to “clean” the money and make it appear as if it came from a legitimate source. Terrorist financing is knowingly providing material support, such as monetary instruments, financial securities or financial services, to individuals associated with a designated terrorist organization, regardless of the legitimacy of the funds. Economic sanctions are financial restrictions imposed by governments or international bodies to try to isolate or impede a specific individual or jurisdiction for some specified purpose.

Money laundering and terrorist financing have global consequences that cannot be countered effectively without the cooperation of governments, international organizations, law enforcement agencies, and financial institutions. Payoneer is required to conduct due diligence on its customers and business partners for money laundering or terrorist risks in order to allow them to continue participating in the system.

Every Payoneer employee must be alert to possible money laundering or terrorist financing situations. If you suspect that Payoneer products or systems are being used for money laundering purposes, it is your responsibility to report your suspicions to the Chief Legal and Regulatory Officer, Chief Compliance Officer, Vice President of Internal Audit, or a Money Laundering Reporting Officer. For more information, employees should review Payoneer’s Anti-Money Laundering Policy.

6. Antitrust and Competition Laws

Payoneer is committed to competing lawfully, ethically and fairly in the marketplace based on the merits of our products and services. In the United States and many other countries, we are subject to antitrust and competition laws and regulations designed to protect the competitive process and prevent anticompetitive conduct. The antitrust laws prohibit agreements among competitors on such matters as prices, terms of sale to customers and allocating markets or customers. Antitrust laws can be very complex, and violations may subject the Company and its employees to criminal sanctions, including fines, jail time and civil liability.

Many situations create the potential for unlawful anticompetitive conduct, or the appearance of impropriety, and should be avoided. These include:

- Agreements with competitors about pricing or pricing policies, allocating clients, products, services, territories or markets, or to limit the production or sale of products, product lines or services;
- Communication with competitors on competitively sensitive topics such as prices, pricing policies, costs, marketing and investment strategies, or proprietary or confidential information in any form (including discussions, informal conversations, emails, and other contacts) or in any setting (including at social gatherings and meetings of trade and professional associations);
- Attempts by business partners, customers or suppliers or potential business partners, customers or suppliers to preclude Payoneer from doing business with, or contracting with, another business partner, customer or supplier.
- Attempts by Payoneer to preclude its business partners, customers or suppliers from dealing

with a competitor of Payoneer where such conduct may foreclose the competitor from the marketplace.

If any person tries to discuss with you subjects that you think may be anticompetitive, you should immediately stop the conversation and report the matter to the Chief Legal and Regulatory Office.

7. Confidentiality

All Payoneer directors and staff must maintain the confidentiality of confidential information entrusted to them by Payoneer or its business partners, customers and other parties in accordance with laws, regulations, contracts, and applicable policies. Confidential information is all non-public information that might provide Payoneer with a competitive advantage, or could be harmful or cause legal exposure to the Company, its customers or its suppliers if disclosed without authorization. Confidential information includes personal account information of cardholders as well as intellectual property (such as trade secrets, patents, trademarks and copyrights), business, marketing and service plans, databases, account or financial records, salary and benefits information, customer, employee and suppliers lists, unpublished financial or pricing information, and any other unpublished data and reports.

You may not disclose any confidential information to anyone outside Payoneer, even to members of your own family. Even within our company and among your co-workers, you must share confidential information only on a need-to-know basis. You should always consult with the Chief Legal and Regulatory Officer before disclosing any such information, even if you believe disclosure might be authorized. You are responsible for identifying and labeling confidential information with the appropriate classifications. Unauthorized use or distribution of proprietary information violates Company policy and could be illegal. Such use or distribution could result in negative consequences for both the Company and the individuals involved, including potential legal and disciplinary actions. We respect the property rights of other companies and their proprietary information and require our employees to observe such rights.

The obligation to preserve confidential information extends to external party information received under nondisclosure restrictions and continues even after employment ends. You must return all proprietary information in your possession upon leaving the Company.

The provisions of this Section 7 are qualified in their entirety by reference to Section 25.

8. Conflicts of Interest

All employees have a duty of loyalty to Payoneer and have an obligation to act in the best interest of the Company. All employees should endeavor to avoid situations that present a potential or actual conflict or the appearance of conflict between their own interests and their responsibilities to Payoneer or its clients. A "conflict of interest" occurs when a person's private interest interferes in any way, or even appears to interfere, with the interest of the Company, including its subsidiaries and affiliates, or whenever the prospect of direct or indirect personal gain may influence or appear to influence our judgment or actions while conducting company business. A conflict of interest may arise when an employee takes an action or has an interest that may make it

difficult for him or her to perform his or her work objectively and effectively. Conflicts of interest may also arise when an employee (or his or her family members) receives improper personal benefits as a result of the employee's position in the Company. The appearance of a conflict of interest can be just as damaging to Payoneer's brand and reputation as an actual conflict of interest. All employees must follow basic conflict of interest principles by avoiding circumstances that could impair objectivity in performing Payoneer job duties, cause favoritism to outside organizations or individuals, interfere with the performance of Payoneer job duties, or damage the reputation of Payoneer's business or brand. Examples of when a conflict situation may arise include:

- Doing business with family or friends, either within Payoneer or through vendors, clients or other business partners (e.g., directing business to a supplier owned or managed by, or which employs, a relative or friend);
- Receiving or giving personal benefits such as gifts or entertainment of more than modest value or personal discounts (if such discounts are not generally offered to the public) from a potential or existing vendor, business partner, competitor or customer, as a result of your position in the Company;
- Working for a competitor, vendor, business partner or customer while employed at Payoneer;
- Having a significant financial interest, such as an investment in a competitor, vendor, businesspartner or customer of Payoneer; or
- Exercising fiduciary responsibility on the Board of an outside organization (for-profit or nonprofit) that does business with Payoneer; or
- Having an interest in a transaction involving the Company, a competitor, a customer or supplier (other than as an employee of the Company and not including routine investments in publicly traded companies);
- Competing with the Company for the purchase or sale of property, products, services or other interests; or
- Receiving loans or guarantees of personal obligations as a result of your position with the Company, or extending such loans or guarantees on behalf of Payoneer, to other directors or staff or their family members.

When faced with a potential conflict of interest, ask yourself:

- Would this activity create or be perceived by others to create an incentive to benefit myself, my friends or my family, or an associated business at the expense of Payoneer?
- Would this harm my reputation, negatively impact my ability to do my job, or potentially harm Payoneer?
- Would this embarrass Payoneer or me if it showed up on the front page of a newspaper or in a blog?

If the answer to any of these questions is "yes," the relationship or situation may create a conflict of interest, and you should avoid it. Directors shall disclose and resolve potential conflicts of interest in accordance with procedures established by the Audit Committee of the Board of Directors, and the Company's Related Party Transaction Policy.

Conflicts of interest may not always be clear-cut, so if you have a question or know of actions that may involve a conflict of interest, you should contact the Chief Legal and Regulatory Officer.

In order to avoid conflicts of interests, executive officers and directors must disclose to the Chief Legal and Regulatory Officer any material transaction or relationship that reasonably could be expected to give rise to such a conflict. Conflicts of interests involving the Chief Legal and Regulatory Officer and directors shall be disclosed to the committee of the Board of Directors with responsibility for corporate governance.

9. Corporate Opportunities

All employees owe a duty to Payoneer to advance its legitimate interests when the opportunity to do so arises. Employees are prohibited from taking for themselves personally business opportunities that are discovered through the use of corporate property, information or position without the consent of the Board of Directors. No employee may use corporate property, information or position for personal gain, nor compete with Payoneer directly or indirectly. Competing with the Company may involve engaging in the same line of business as the Company, or any situation where the employee takes away from the Company opportunities for sales or purchases of products, services or interests.

10. Data Privacy

Non-public, personally-identifiable information is one of Payoneer's most sensitive assets. Payoneer's failure to maintain the privacy of such information could cause significant damage to Payoneer's business and reputation. As a result, non-public, personally-identifiable information of employees, customers, business partners, contractors, consultants and other individuals should be collected, stored, transmitted, accessed and used only in accordance with Payoneer's Data Governance Policy and in compliance with applicable law and Employees should protect Payoneer's information at all times in accordance with Payoneer's Data Governance Policy. Access to employees' (including former employees) emails may be required in certain circumstances, in accordance with Payoneer's Data Governance Policy.

For more information, employees should review Payoneer's Privacy Policy and Data Governance Policy.

Government authorities or lawyers for outside parties may seek to contact you directly with respect to audits, reviews, investigations or other claims against Payoneer. All such inquiries must be referred to the Chief Legal and Regulatory Officer before any information or response is provided. In addition, you may receive requests from various government authorities, lawyers or other parties for access to Payoneer transaction data or other information assets. All requests for Payoneer information assets must be referred to the Chief Legal and Regulatory Officer or the Chief Compliance Officer before any information or response is provided to the requesting authority. This ensures that such inquiries are handled in accordance with relevant legal and data protection requirements.

11. Equal Opportunity

The diversity of Payoneer's staff is a tremendous asset. We are proud of and value our differences and understand that diversity and inclusion are good for business and make our company stronger.

We are firmly committed to providing equal opportunity in all aspects of employment and will not tolerate any form of discrimination or harassment in the workplace on the basis of race, color, creed, national origin, religion, age, sex, sexual orientation, gender, gender identity, gender expression, disability, marital or veteran status, condition of pregnancy or any other characteristic protected by applicable law. All employees are required to comply with this policy. Should any Payoneer employee feel that they have not been treated fairly or with dignity, they should immediately contact the Chief Legal and Regulatory Officer or Vice President of Internal Audit. All complaints will be investigated promptly.

We foster an environment where employees are comfortable asking questions and taking an active role in understanding, discussing and exploring issues. In this way, we can be sure to identify and address issues or concerns even before they grow into larger problems. Working together to maintain an environment that fosters trust and that empowers us to take initiative and hold ourselves accountable is an essential part of the Payoneer culture. Our continuing success as individuals, colleagues, and a company depends on all of us treating each other with respect and upholding the highest professional and ethical standards.

12. Harassment-Free Workplace

We strive to create a work environment free of discrimination and harassment. We do not tolerate bullying, abuse or any behavior that interferes with someone's work or that creates a hostile work environment. No matter what form harassment takes—whether physical, sexual, verbal or non-verbal, in person, via email, over the phone or on the internet—it is unacceptable.

We each have a responsibility to recognize harassment so that we can report it promptly when we see it. Harassment is offensive conduct that interferes with an employee's ability to work, or creates a hostile or intimidating work environment. Harassment can involve sexual conduct or references to a personal characteristic. Examples include racial slurs, off-color jokes, unwelcome sexual advances, or displaying or transmitting suggestive or sexually explicit images. Harassment can occur between members of the same sex or the opposite sex; between vendors, contractors, or employees; and in the office or at off-site work-related events.

We speak up if we suspect discrimination, harassment or other inappropriate workplace behavior. We strongly encourage you to immediately report any incidents to a manager, Human Resources, Legal or by calling the Ethics Voicemail Box or using the [Web Form](#) (as described in [Appendix A](#) hereto), and we will ensure that any complaints are quickly and thoroughly investigated and to take appropriate action. Payoneer investigates all reports of harassment and keeps these reports as confidential to the extent consistent with Payoneer's ability to conduct a full and fair investigation and to comply with its legal obligations and policies.

13. Fair Dealing

We seek to outperform our competition fairly and honestly. We seek competitive advantages through superior performance, never through unethical or illegal business practices. Stealing proprietary information, gathering competitive intelligence in a manner that is unlawful or unethical, possessing trade secret information that was obtained without the owner's consent, or inducing such disclosures by past or present employees of other companies, is strictly prohibited. Employees should endeavor to respect the rights of and deal fairly with Payoneer's business

partners, customers, suppliers, competitors, the public and other employees at all times and in accordance with ethical business practices. No employee should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other intentional unfair-dealing practice.

The purpose of business entertainment and gifts in a commercial setting is to create goodwill and sound working relationships, not to gain unfair advantage with clients. No business gift or entertainment should ever be offered, given, provided or accepted by any employee, family member of an employee, or agent unless it:

- Is given to a non-government employee;
- Is given infrequently;
- Is not a cash or cash equivalent gift (other than approved Payoneer cards);
- Is consistent with customary business practices;
- Is objectively of modest value under the circumstances;
- Cannot be construed as a bribe, a payoff or as otherwise intended to inappropriately influence a business decision; and
- Does not violate any laws, regulations or applicable policies.

Gifts or entertainment in any form that would likely result in a feeling or expectation of personal obligation should not be extended or accepted. Practices that are acceptable in a commercial business environment may be against the law or the policies governing federal, state or local government employees. Therefore, no gifts or business entertainment of any kind may be given to any government employee without the prior approval of a manager/supervisor or the Legal Department. Except in certain limited circumstances, the Foreign Corrupt Practices Act ("FCPA") prohibits giving anything of value directly or indirectly to any "foreign official" for the purpose of obtaining or retaining business (please see Section 3 above for further details). Please discuss with your manager, the Legal Department, the Compliance Department or the VicePresident of Internal Audit, any business entertainment or gifts which you are not certain are appropriate.

14. Quality of Public Disclosures

The Company has a responsibility to provide full and accurate information in our public disclosures, in all material respects, about the Company's financial condition and results of operations. Our reports and documents filed with or submitted to the Securities and Exchange Commission and our other public communications shall include full, fair, accurate, timely and understandable disclosure, and the Company has established a Disclosure Committee consisting of senior management to assist in monitoring such disclosures.

15. Health and Safety

The Company is committed to conducting its business in compliance with all applicable environmental and workplace health and safety laws and regulations. Payoneer strives to provide each employee with a safe and healthy work environment. All employees have the responsibility for maintaining a safe and healthy workplace by following security, health and safety rules. Suspicious or criminal activity, accidents, injuries and unsafe equipment, practices or conditions should be immediately reported to your manager and the general manager of your office location.

Performing work while under the influence of alcohol, illegal drugs or improperly used prescription medication is unsafe and puts us all at risk. This is prohibited, and working under the influence of such substances will not be tolerated. The only exception to this rule is when alcohol is used responsibly and in moderation at business dinners and at certain authorized Payoneer events. Violence and threatening behavior are not permitted. Any acts or threatened acts of violence must be reported immediately to your manager and Chief Legal and Regulatory Officer.

16. Insider Trading

Payoneer is committed to adhering to the securities laws of the United States and other applicable countries. These laws prohibit certain transactions involving securities (e.g., purchases or sales of Payoneer's stock or restricted stock, exercise and sale of Payoneer stock options or RSUs) by persons who are aware of material information about Payoneer that is not generally known by or available to the public. These laws also can, in many circumstances, prohibit persons who are aware of such material non-public information from disclosing this information to others. Payoneer and its directors, officers and executive management may also be subject to liability if they fail to take reasonable steps to prevent insider trading by Payoneer's personnel.

Furthermore, Using non-public, Company information to trade in securities, or providing a family member, friend or any other person with a "tip", is illegal. All non-public, company information should be considered inside information and should never be used for personal gain. No director, officer or employee of the Company who, in the course of working for the Company, learns of any material, nonpublic information about a company with which the Company does business (e.g., a customer, supplier or other party with which the Company is negotiating a major transaction, such as an acquisition, investment or sale), may trade in that company's securities until the information becomes public or is no longer material. This remains true even in the event that you are no longer working with or for the Company.

You are required to familiarize yourself and comply with the Company's Policy Against Insider Trading, copies of which are distributed to all employees and are available from the Legal Department or on [Payoneer Connect](#). You should contact the Legal Department with any questions about your ability to buy or sell securities.

17. Protection and Proper Use of Company Assets

Part of working ethically and with integrity involves protecting Payoneer's physical assets as well as our intangible assets and trade secrets, including our brand, reputation and proprietary or confidential information. Payoneer assets should be used responsibly. All employees have an obligation to safeguard Payoneer's assets, protect them from loss and ensure their efficient use. Theft, carelessness and waste have a direct impact on Payoneer's profitability. Any suspected incident of misuse, loss or theft should be immediately reported for investigation to the Chief Legal and Regulatory Officer. Payoneer equipment should not be used for non-Payoneer business, though incidental personal use may be permitted.

The obligation of Payoneer directors and staff to protect company assets extends to confidential information, as discussed in Section 7 above. Unauthorized use or distribution of this information would violate Payoneer policy. It could also be illegal and result in civil or even criminal penalties.

You must also respect the valid intellectual property rights of others. Everyone should ensure that Payoneer property under their control is properly used and protected by adequate controls and safeguards.

Your Payoneer-issued (desktop and/or laptop) personal computer (PC) as well as any other Payoneer devices or systems to which you have access (including without limitation, emails and storage applications) are the property of Payoneer and are intended primarily for business use. Limited, appropriate, personal use of your PC or other Payoneer-issued devices is acceptable, if it does not interfere with your work or violate Payoneer policies or standards. We should also never use our company computers or network systems for inappropriate conduct.

18. Record Keeping

Payoneer requires honest and accurate recording and reporting of information, hours worked and expenses in order to make responsible business decisions. Many employees regularly use business expense accounts, which must be documented and recorded accurately. If you are not sure whether a certain expense is legitimate, ask your manager or a member of the Finance team.

Purposely misrepresenting information or activities on company documents and reports is a serious violation of policy, and may violate the law. This could have serious consequences for you individually as well as for the company. Intentional misrepresentation or falsification of records will result in disciplinary action up to and including termination, and may potentially involve additional penalties as well. When in doubt, it is always better to ask before taking action.

All of Payoneer's books, records, accounts, and financial statements:

- Must be maintained in reasonable detail;
- Must appropriately reflect Payoneer's transactions;
- Must conform to applicable legal requirements; and
- Must be accurately maintained in accordance with Payoneer's system of internal controls.

Business records and communications often become public, and we should avoid exaggeration, derogatory remarks, guesswork or inappropriate characterizations of people and companies that can be misunderstood. This applies equally to e-mail, internal memos and formal reports. Records should always be retained or destroyed according to applicable policies. In the event of litigation or governmental investigation, please consult with the Legal Department regarding special record retention requirements.

Employees should not engage in any transaction where there is reason to believe that the objective of the customer, business partner or other party is to achieve misleading earnings, revenue, cash flow or balance sheet effect in its financial statements.

19. External Communications

We need to speak with "one voice" to the community outside of Payoneer. Communicating consistent and accurate information to the public, our customers, potential customers, business partners and investors is vital to our reputation and is required to meet regulatory and legal

obligations. Inaccurate statements can create serious risks for the Company. Only authorized Payoneer representatives can speak on behalf of Payoneer to the press or at external events, conferences, industry tradeshows, or forums. If you receive an inquiry from the media, you are not authorized to speak or provide any answers or information on behalf of Payoneer without first consulting with the VP Marketing. Inquiries from the investment community must be referred to the Chief Financial Officer.

As a company, we encourage communication among our employees, customers, partners, and others with Web logs (blogs), social networks, discussion forums, wikis, video, and other social media. This can be a great way to stimulate conversation and discussion. The Payoneer Social Media Policy sets forth the guidelines for employee participation in social media and encourages employees to act responsibly, respectfully and transparently when using social media.

20. Payoneer Products and Services

Given that a significant number of employees and staff have access to critical Payoneer systems (i.e., BackOffice), servers, operating and financial accounts, as well as to reduce the opportunity for internal fraud or impropriety generally, no Payoneer director, officer, employee, contractor, consultant or temporary staff person, nor family members who share the same household with the foregoing, may register for or use any Payoneer product or service, including but not limited to, a Payoneer card (excluding cards issued by Israel Post Bank and cards issued through David Shield Passportcard programs) or Payoneer virtual account; provided, however, that upon receiving advance written approval from the Chief Compliance Officer, such persons may use Payoneer's products and services in certain prescribed situations. Requests for advance approval should be submitted to the Internal Fraud Monitoring Team.

21. Political Contributions and Activities

Any political contributions made by or on behalf of the Company and any solicitations for political contributions of any kind must be lawful and in compliance with Company policies. This policy applies solely to the use of Company assets and is not intended to discourage or prevent individual employees from making political contributions or engaging in political activities on their own behalf. No one may be reimbursed directly or indirectly by the Company for personal political contributions.

22. Reporting any Illegal or Unethical Behavior

Payoneer staff are encouraged to talk to any of their managers, senior managers, Legal or Internal Controls about any observed, or suspected, illegal or unethical behavior or Code-related policy violations and when in doubt about the best course of action in a particular situation. Employees will have the opportunity to ask confidential follow-up questions and be advised of report status. Payoneer does not tolerate retaliation against anyone who reports observed, or suspected, illegal or unethical behavior, or Code-related policy violations, in good faith.

23. Waivers of the Code of Conduct and Ethics

Requests for waivers of this Code by a staff member must be approved by the Chief Legal and

Regulatory Officer or Chairman of the Audit Committee. Waivers for executive officers or directors may be made only by the Board of Directors or an authorized committee of the Board of Directors, or as otherwise required by law. Amendments to this Code must be approved by the Nominating and Corporate Governance Committee.

24. Complying with the Code

We all must work to ensure compliance with this Code and prompt and consistent action against any violations. The Code will be strictly enforced, and violations will be dealt with immediately, including by subjecting persons who violate its provisions to corrective and/or disciplinary action such as dismissal or removal from office. Violations of the Code that involve illegal behavior will be reported to the appropriate authorities.

However, in some situations it is difficult to know the right thing to do, and you may be required to exercise your judgment or to make difficult decisions. As we cannot anticipate every situation that will arise, it is important that we have a way to approach a new question or problem. These are the steps to keep in mind:

- *Always ask first, act later.* If you are unsure about what to do in any situation, seek guidance before you act.
- *Make sure you have all the facts.* In order to reach the right solutions, you must be as fully informed as possible.
- *Ask yourself: What specifically am I being asked to do? Does it seem unethical or improper?* This will enable you to focus on the specific question you are faced with and the alternatives you have. Use your judgment and common sense; if something seems unethical or improper, don't take the risk of doing it.
- *Clarify your responsibility and role.* In most situations, there is shared responsibility. Are your colleagues informed? It may help to get others involved and discuss the problem.
- *Discuss the problem with your manager.* This is the basic guidance for most situations. In many cases, your manager will be more knowledgeable about the question, and will appreciate being brought into the decision-making process. Remember that it is your manager's responsibility to help solve problems.
- *Seek help from leaders other than your manager.* In situations where it may not be suitable to discuss an issue with your manager, or where you do not feel comfortable approaching your manager with your question, discuss it with Legal or Internal Controls.
- *You may make good faith reports about ethical violations in confidence and without fear of retaliation.* Payoneer does not permit retaliation of any kind against employees for good faith reports of ethical violations.

If you become aware of a violation or potential violation of the Code or accounting standards or controls, you should promptly report your concern to the Chairman of the Audit Committee of the Board of Directors, the Chief Legal and Regulatory Officer or any other attorney in the Legal Department, the Chief Compliance Officer or the Vice President of Internal Audit.

Any concerns about a violation of ethics, laws, rules, regulations or this Code by the CEO or any senior financial officer should be reported promptly to the Chief Legal and Regulatory Officer, and the Chief Legal and Regulatory Officer shall notify the Nominating and Corporate

Governance Committee of any violation. Any such concerns involving the Chief Legal and Regulatory Officer should be reported to the Nominating and Corporate Governance Committee. Reporting of such violations may also be done anonymously through the Ethics Voicemail Box or [Web Form](#). An anonymous report should provide enough information about the incident or situation to allow the Company to investigate properly. If concerns or complaints require confidentiality, including keeping an identity anonymous, the Company will endeavor to protect this confidentiality, subject to applicable law, regulation or legal proceedings.

The Company recognizes the need for this Code to be applied equally to everyone it covers. The Chief Legal and Regulatory Officer of the Company will have primary authority and responsibility for the enforcement of this Code, subject to the supervision of the Nominating and Corporate Governance Committee, or, in the case of accounting, internal accounting controls or auditing matters, the Audit Committee of the Board of Directors, and the Company will devote the necessary resources to enable the Chief Legal and Regulatory Officer to establish such procedures as may be reasonably necessary to create a culture of accountability and facilitate compliance with the Code. Questions concerning this Code should be directed to the Legal Department.

The provisions of this Section 24 are qualified in their entirety by reference to Section 25.

25. Reporting Violations to a Governmental Agency

You have the right to not be retaliated against for reporting, either internally to the Company or to any governmental agency or entity or self-regulatory organization, information which you reasonably believe relates to a possible violation of law. It is a violation of federal law to retaliate against anyone who has reported such potential misconduct either internally or to any governmental agency or entity or self-regulatory organization. Retaliatory conduct includes discharge, demotion, suspension, threats, harassment, and any other manner of discrimination in the terms and conditions of employment because of any lawful act you may have performed. It is unlawful for the Company to retaliate against you for reporting possible misconduct either internally or to any governmental agency or entity or self-regulatory organization.

Your rights and remedies as a whistleblower protected under applicable whistleblower laws, including a monetary award, if any, may not be waived by any agreement, policy form, or condition of employment, including by a predispute arbitration agreement.

26. Conclusion

Payoneer expects that every employee, at every level, will strive to conduct him- or herself with integrity. It is hoped that the Code will help you identify potential integrity issues, and give you guidance on how to deal with such situations. Remember, if you are ever uncertain about how to act, please seek advice from your manager, an attorney from the Legal Department.

Key Contacts

Avi Zeevi
Chairman of the Audit Committee of the Board of Directors
aviz@viola.vc

Tsafi Goldman
Chief Legal and Regulatory Officer
tsafigo@payoneer.com
Israel Office: 073- 263-3490

Jani Gode
Chief Compliance Officer
janigo@payoneer.com
US Office: 1-646-588-2783

Sharon Ben Yaakov–Ilani
Vice President of Internal Audit
sharonbe@payoneer.com
Israel Office: 073-2633-567

Amanda Kosonen
Global Regulatory Counsel
amandako@payoneer.com
US Office: 1-646-588-2865

Exhibit A

Payoneer Whistleblower Claims Procedures

OVERVIEW AND PURPOSE

These procedures establish guidelines and processes for handling whistleblower claims. By appropriately responding to allegations by employees, suppliers, customers or contractors that the Company is not meeting its legal and ethical obligations, the Company can better support an environment where compliance is the norm. An appropriate response includes protecting those who step forward in good faith from retaliation while at the same time ensuring that the targets of any allegations have an opportunity to present relevant evidence and understand the nature of the allegations.

This policy document details what actions should be taken by:

- Individuals, who have knowledge of any facts or indications of serious breaches of policy or the law.
- Company management when whistleblower allegations are made.

KEY CONTACTS

Whistleblower claims and allegations may be communicated to any one or more of the following Company representatives:

- (i) Chairman of the Audit Committee of the Company's board of directors
 - Avi Zeevi – aviz@viola.vc
- (ii) Chief Legal and Regulatory Officer
 - Tsafi Goldman – tsafigo@payoneer.com, Office phone: 073 263 3490
- (iii) Vice President of Internal Audit
 - Sharon Ben Yaakov-Ilani – sharonbe@payoneer.com, Office phone: 073-2633-567
- (iv) Global Regulatory Counsel
 - Amanda Kosonen – amandako@payoneer.com, Office phone: 646-588-2865
- (v) Anonymously and confidentially via the:
 - Ethics Voicemail box
 - +1-332-282-2380
 - +972-77-220-3382
 - Submitting a report to the [Ethics Web Form](#)

SCOPE

This policy applies to all Company employees and contractors and governs procedures that must be followed when allegations of impropriety or irregularity are made by a whistleblower and such allegations (i) regard Code of Conduct violations, (ii) regard accounting, internal accounting controls, or auditing matters, (iii) could cause serious damage to the Company's brand or reputation or, (iv) could result in a material liability to the Company, including, without limitation, the following:

- fraud or deliberate error in the preparation, evaluation, review or audit of any financial statement of the Company;
- fraud or deliberate error in the recording and maintaining of financial books and/or records of the Company;
- deficiencies in or noncompliance with the Company's internal controls;
- misrepresentation or false statement to or by a senior officer or accountant regarding a matter contained in the financial records, financial reports or audit reports of the Company;
- any attempts to mislead or improperly influence the Company's independent auditor in the course of the performance of their audit;
- deviation from full and fair reporting of the Company's financial condition, such as material misrepresentations or omissions with respect to the Company's business, financial condition, results of operations or cash flows, in public disclosures of the Company's financial position and prospective reports;
- improper expenditure of Company funds;
- improper use of Company property (including disclosure of proprietary information); or
- use of non-public Company or client information to trade in securities.

Allegations of impropriety outside the scope of this policy should still be reviewed by the Chief Legal and Regulatory Officer to determine an appropriate course of action.

KEY DEFINITIONS

"Whistleblower" means an individual who brings to the attention of Company management an allegation of impropriety within the Company that has not been resolved to the satisfaction of the individual and that prevents the Company from meeting its legal obligations or from complying with generally accepted accounting principles.

"Target" means a person potentially implicated in the whistleblower allegations.

ROLES & RESPONSIBILITIES

Manager Responsibilities

Managers at all levels are responsible for continually emphasizing integrity as a standard of performance for all employees.

Managers who are apprised by employees, suppliers, customers or contractors that the Company is allegedly not meeting its legal obligations should contact the Chief Legal and Regulatory Officer, the Chairman of the Audit Committee or Vice President of Internal Audit so that an appropriate investigation can be conducted.

Employee Responsibilities

Employees suspecting serious breaches of policy or the law should report them immediately to their leaders. If it is impractical or inappropriate for the employee to notify their immediate supervisor the employee may contact any one or more of the following: the Chairman of the Audit Committee, the Chief Legal and Regulatory Officer, or the Vice President of Internal Audit. Contact can be made via telephone or email. The Company encourages employees who wish to report potential wrongdoings to provide only objective evidence to support their allegations.

The name of a whistleblower who presents allegations may not be disclosed directly to the target(s) of the allegations or management unless authorized by the whistleblower except in those limited instances when the Company has a duty to inform, e.g., imminent threat of serious harm. In addition, regardless of what channel is notified of the allegations, the name of the whistleblower may not be disclosed to the target(s) in those jurisdictions that prohibit such a disclosure. In those instances when information needs to be disclosed, such disclosure will only be to those who have a need to know and only to the extent necessary.

Employees or contractors who have reason to believe that a serious breach of policy or law has occurred must retain all documents that could be relevant to an investigation of the matter.

POLICY REQUIREMENTS

It is Company policy to closely scrutinize and appropriately respond to allegations by employees, suppliers, customers or contractors that the Company is not meeting its legal or ethical obligations or complying with generally accepted accounting principles when such allegations (i) regard accounting, internal accounting controls, or auditing matters, (ii) could cause serious damage to the Company's brand or reputation or, (iii) could result in a material liability to the Company.

Investigating Whistleblower claims

The person receiving the whistleblower information should contact the Chairman of the Audit Committee, the Chief Legal and Regulatory Officer, or the Vice President of Internal Audit. As soon as one of the designated contacts has been informed, investigators should coordinate any further action through the Chief Legal and Regulatory Officer. The Chief Legal and Regulatory Officer will determine how to address the allegations, including whether any matter falling within the scope of this policy should be reported to the Board of Directors, and whether the complaint pertains to an accounting or auditing matter, or whether it pertains to violations of the Code or other relevant matters.

Target employees should not be questioned, terminated, disciplined or otherwise advised of investigations until management is instructed to do so.

In the event that a complaint involves or implicates the Chairman of the Audit Committee, the Chief Legal and Regulatory Officer, or the Vice President of Internal Audit, such person will promptly recuse themselves from the investigation and inform the Audit Committee in writing. The Audit Committee will thereafter promptly appoint impartial attorneys to investigate the complaint. The impartial attorneys will conduct an investigation of the complaint and report their conclusion to the Audit Committee consistent with this policy.

Complaints relating to accounting and auditing matters will be reviewed under Audit Committee direction and oversight by the Chief Legal and Regulatory Officer, Vice President of Internal Audit or such other persons as the Audit Committee determines to be appropriate. Complaints relating to violations of the Code or any other matters will be reviewed initially by the Chief Legal and Regulatory Officer. The Chief Legal and Regulatory Officer may delegate the oversight of any complaint to Internal Audit or such other persons as the Chief Legal and Regulatory Officer determines to be appropriate. This direction may include the assignment of an auditor, special agent or compliance personnel to make a thorough examination. In limited situations, outside counsel, outside auditors or others may be engaged to conduct the investigation.

After initial review, the Audit Committee or Chief Legal and Regulatory Officer, as applicable, will

determine whether the matter warrants an investigation and will oversee any such investigation. If the matter appears to be significant, the Chief Legal and Regulatory Officer will discuss at any time the concerns raised with the Audit Committee or the Chairman of the Audit Committee.

The person(s) authorized to conduct the investigation will report to the Audit Committee in a timely manner all findings of fact, conclusions and proposed recommendations for remedial actions, if any.

Prompt and appropriate corrective action will be taken as and when warranted in the judgment of the Audit Committee or the Chief Legal and Regulatory Officer, as applicable and as appropriate under the circumstances.

The Company will not directly or indirectly, discharge, demote, suspend, threaten, harass or in any manner discriminate against any employee who filed a complaint on a non-anonymous basis (or whose identity came to the attention of the persons involved in the investigation), in his or her terms and conditions of employment based upon any lawful complaint made by such employee in good faith with respect to accounting and auditing matters or violations of the Code or other relevant matters under the scope of this policy.

Confidentiality will be maintained to the fullest extent possible, unless otherwise consented to by the employee who filed the complaint on a non-anonymous basis, as may be necessary to conduct a thorough investigation or as required to be disclosed by law.

In conducting an investigation, precautions should be taken to safeguard against unfounded, inaccurate or unwarranted accusations. An investigation should be conducted, including interviewing the employee, supplier, customer or contractor making the allegations and the target. The target of any allegations should have an opportunity to present relevant evidence and understand the nature of the allegations. However, the target should not be notified of the allegations prior to the adoption of any protective measures necessary to prevent the destruction of evidence, should such measures be deemed necessary.

Personal data gathered during the course of the investigation will be handled in accordance with local data privacy laws but in all instances, information gathered must be kept securely and access to such information should be limited to those who need to know in order to perform their job duties. Data that could identify the whistleblower or the target should not be retained any longer than is necessary for the Company to satisfy its legal obligations.

The Audit Committee is responsible for tracking all whistleblower claims within the scope of this policy and for ensuring that the tenets of the policy are followed. Copies of complaints and such log will be maintained in accordance with the Company's document retention policy.

The Company, as directed by the Chief Legal and Regulatory Officer, will make every effort to cooperate with law enforcement authorities. Law enforcement authorities should not be contacted by the Company in whistleblower situations until instructions have been received from the Chief Legal and Regulatory Officer. An exception would be in the rare instance when, for example, a theft or similar crime is discovered in the process of being committed and authorities have to be contacted to prevent the crime from being perpetrated.

Disciplinary Measures Against Target

Once investigated, a decision on what course of action to take based on the findings of the investigation must be approved by the Chief Legal and Regulatory Officer who will apprise the Audit Committee as appropriate.

Disciplinary measures against the target will depend on the circumstances and will be applied in consultation with Human Resources and the Chief Legal and Regulatory Officer. Consideration will be given to whether or not a violation is intentional, as well as to the level of good faith shown by a target in cooperating with any resulting investigation or corrective measures.

Retaliation against Whistleblowers

Every employee has the right to not be retaliated against for reporting, either internally to the Company or to any governmental agency or entity or self-regulatory organization, allegations of impropriety that fall within the scope of this policy or other violation of the law, and which the employee reasonably believes in good faith to be true.

It is unlawful and a violation of federal law to retaliate against anyone who has reported such potential misconduct in good faith either internally or to any governmental agency or entity or self-regulatory organization. Retaliatory conduct includes discharge, demotion, suspension, threats, harassment, and any other manner of discrimination in the terms and conditions of employment because of any lawful act the employee may have performed.

The Company cannot require an employee to withdraw reports or filings alleging possible violations of federal, state or local law or regulation, and may not offer an employee any kind of inducement, including payment, to do so.

An employee's rights and remedies as a whistleblower protected under applicable whistleblower laws, including a monetary award, if any, may not be waived by any agreement, policy form, or condition of employment, including by a predispute arbitration agreement.

Even if an employee has participated in a possible violation of law, he or she may be eligible to participate in the confidentiality and retaliation protections afforded under applicable whistleblower laws, and may also be eligible to receive an award under such laws.

Please note, that allegations that are not brought forth in good faith are a misuse of the whistleblower process and may result in disciplinary action against the whistleblower.

The Audit Committee may revise or amend this policy as necessary or appropriate.