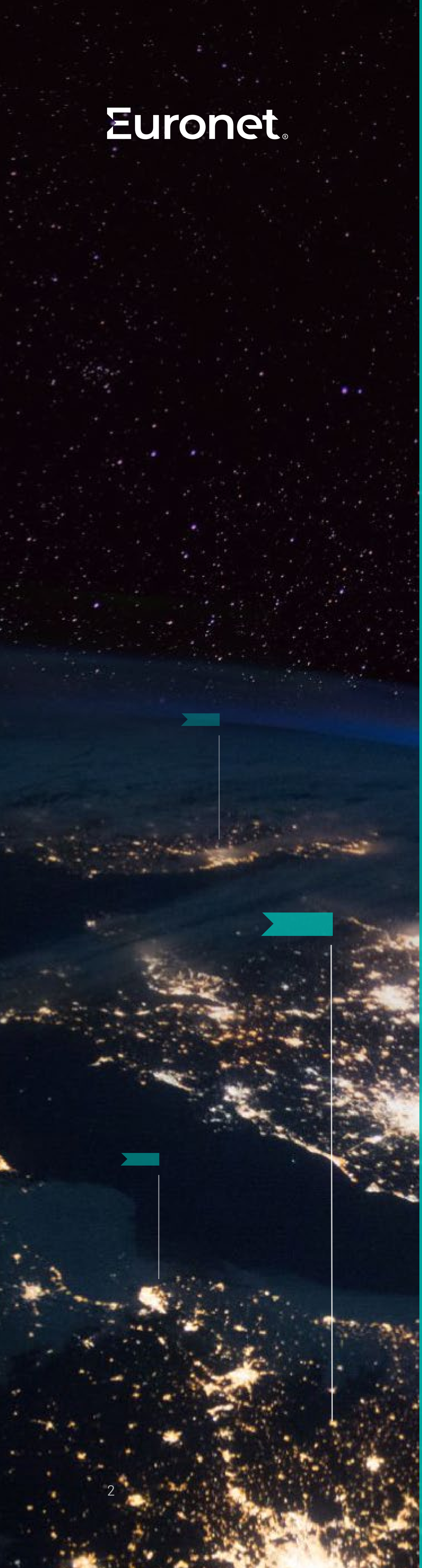
Euronet

2026 Global Policies & Statements



Contents

About the Flags
As part of the Euronet logo, the Euronet flag represents our global coverage in 200 countries and territories. In this report, we use the flag to symbolize the expansive geographic reach of our payments network.

Euronet Standards

Reporting Procedures

Any employee who believes he or she has experienced or witnessed any conduct that is in violation of this policy should report that concern to a supervisor, Human Resources representative, the Company's General Counsel or through the Global Ethics Hotline immediately. These are the individuals authorized by this policy to receive complaints on behalf of the Company. This policy does not require reporting harassment to any individual who is creating the harassment.

Complaints may be made orally or in writing. If a complaint is made orally, the employee may be asked for a written statement during the investigation. All complaints, to the extent possible, should include dates, times, location, details of the incident(s), names of the individuals involved and the names of witnesses to the incident(s). Any supervisor who is aware of conduct inconsistent with this policy or who receives or learns of a report of conduct inconsistent with this policy must report such conduct immediately to Human Resources.

Responding to Complaints

All reports describing conduct that is inconsistent with this policy will be investigated promptly and thoroughly. Employees are required to cooperate in investigations. The Company is committed to maintaining confidentiality to the extent possible. The Company will take all reasonable measures to ensure that the situation is divulged only to those with a need to know.

Corrective Action

We will not tolerate any harassment or discrimination in violation of this policy. If an investigation reveals that a violation of this policy or other inappropriate conduct has occurred, then the Company will take corrective action, including discipline, up to and including termination of employment, as is appropriate under the circumstances, regardless of the job positions of the parties involved. The Company may discipline an employee for any inappropriate conduct discovered in investigating reports made under this policy, regardless of whether the conduct amounts to a violation of law. If the person who engaged in conduct in violation of this policy is not a Company employee, then we will take whatever corrective action is reasonable and appropriate under the circumstances.

Retaliation Prohibited

Retaliatory treatment of any employee for reporting discrimination, harassment or other prohibited behavior or for cooperating in a harassment investigation is strictly forbidden. All employees who experience or witness any conduct they believe to be retaliatory should immediately report such conduct to a supervisor, Human Resources representative, the Company's General Counsel or through the Global Ethics Hotline.

Anti-Bribery Policy

Statement of Policy

Euronet Worldwide, Inc., its subsidiaries, and those affiliates over which Euronet Worldwide, Inc. has operational control (collectively, the "Company" or "EWI") prohibit bribery of public officials and corporate representatives in the conduct of its business throughout the world. All Company employees are required to strictly comply with the United States Foreign Corrupt Practices Act (the "FCPA"), the U.K. Bribery Act and with anti-bribery laws in the countries in which they are operating (collectively "Anti-Bribery Laws"). Anti-Bribery Laws prohibit the bribery of government officials (including officials of designated public international organizations and employees of companies owned or controlled by foreign governments), compliance party candidates or officials, or political parties.

Some Anti-Bribery Laws, including the U.K. Bribery Act, prohibit the bribery of representatives of corporations and other business entities ("corporate representatives"). Bribery can take many forms, including the promise or payment of money or anything else of value (such as "in kind" items, services, lavish gifts or entertainment, or charitable donations, for example). The FCPA also requires that the Company's books, records, and accounts be kept in reasonable detail to reflect the Company's transactions and disposition of assets accurately and fairly.

Bribes Prohibited

Bribes, kickbacks or otherwise giving or promising anything else of value to individual public official(s) or individual corporate representative(s) in an attempt to influence the action or inaction of those individuals for purposes of gaining an improper business advantage (or avoiding a business disadvantage), will not be tolerated and are strictly prohibited. This prohibition extends to payments to consultants, agents or any other intermediary when the employee knows or has reason to believe that some part of the payment or "fee" will be used to bribe or otherwise influence a public official or corporate representative. If any employee is confronted with a demand for a bribe from anyone, that demand must be reported immediately to his or her supervisor and to the Company's General Counsel or Compliance Officer.

Administration of the Policy

The Policy will be administered by the Audit Committee of the EWI Board of Directors, the EWI General Counsel and Compliance Officer. Contact information for those individuals will be provided in the Anti-Bribery Program Compliance Manual (the "Manual").

Policy Manual

EWI management will prepare and maintain the Manual in order to provide specific guidance on the implementation and enforcement of this Policy. The Manual will be distributed to all employees and representatives who have control over any EWI funds or who have responsibility for recording transactions that impact EWI books and records

Accurate Books & Records

The FCPA specifically requires that the Company's books, records, and accounts be kept in reasonable detail to accurately and fairly reflect the Company's transactions and asset dispositions. Therefore, the Company also prohibits:

- Subterfuge of any kind, e.g., the payment of "bonuses" or "success fees" to agents or other third parties for activities that would violate this, Policy.
- Activities intended to circumvent laws using payments to agents, consultants, or subcontractors.
- Mischaracterization or intentional vagueness in recording entries in the books and records of the Company.
- The recording of any false or artificial entries on the books and records of the Company; and
- Creation or maintenance of any assets or liabilities, which are not reflected in the books and records of the Company (so-called "hidden accounts," "slush funds" or "hidden debts").

Exceptions will be made only with the prior written approval of the Company's General Counsel or Compliance Officer.

Facilitating Payments

So-called "grease," "facilitating," or "expediting" payments, known as "Facilitating Payments," are usually modest amounts of money paid to low-ranking officials engaged in ministerial duties for routine governmental actions. These Facilitating Payments are not allowed unless the life, health or safety of an employee is threatened. If such a situation occurs, the person making the payment must contact the Company's General Counsel or Compliance Officer within 48 hours to provide all information requested. Any payment made under these circumstances must be accurately recorded in the Company's books and records.

Legitimate Expenses and Legal Practices Outside the United States

Anti-Bribery Laws contain certain exceptions for conduct which would be illegal regarding an official of the United States but may be permitted under certain circumstances by other governments regarding their officials. For example, in the United States, you may not buy a meal for an official of the United States government, but in other countries such a practice may be lawful, normal, and customary. However, and prior to promising or making any payment or giving anything of value (whether in-kind or otherwise) to a public official or corporate representative in any country, or in the event that questions arise with regard to the proper maintenance of Company books and records, employees must seek the advice of the Company's General Counsel or Compliance Officer ahead of the event or anticipated payment and act accordingly.

Reasonable, bona fide expenditures, such as travel and lodging expenses that are associated with the promotion of a product or service or with the performance of a contract are generally an exception to Anti Bribery Laws. However, prior to promising or making any payment or giving anything of value (whether in-kind or otherwise) to a public official or corporate representative in any country, or in the event that questions arise with regard to the propriety of the expenses, employees must seek the advice of the Company's General Counsel or Compliance Officer ahead of the event or anticipated payment and act accordingly.

You are not required to contact the Company's General Counsel or Compliance Officer in advance if you are hosting reasonable and infrequent meals or entertainment for corporate representatives. Likewise, nominal gifts to corporate representatives, which bear the Company's logo, do not require this step.

Third Party Agents, Consultants and Representatives

Employees must obtain the prior written approval of the Company's General Counsel or Compliance Officer prior to the engagement of attorneys, (excluding Ria or epay agents that are part of their product distribution networks,whose selection in the ordinary course shall be subject to their standard compliance procedures), consultants and other representatives who are outside of the United States or represent the interests of the Company outside of the United States and who have the potential to represent the company before public officials or corporate customers. Prior to approval, all such agents and third parties must be subjected to appropriate due diligence. Any approval is contingent on:

- Positive results from due diligence.
- Having the agent or third party contractually obligated to comply with Anti-Bribery Laws; and
- Presenting documented communications in which Company employees have positively informed the agent or third party of the Company's commitment to comply with Anti-Bribery Laws.

Donations — It is never permissible to provide a donation to improperly influence a government official, or in exchange for any improper favor or benefit. It may, however, be permissible to make donations directly to a government agency (rather than to an individual government official) as part of a charitable effort. Prior approval from the Company's General Counsel is required before making such a donation.

Promoting, Demonstrating, or Explaining Products — It is never permissible to direct promotional expenses or activities to a government official to improperly influence him or her, or in exchange for any improper favor or benefit. In some cases, however, it may be appropriate to direct such expenses to a government official or entity in order to promote, demonstrate, or explain the Company's products and services. Before doing so,Company associates must seek prior approval from the Company's General Counsel.

Hiring or Engaging Government Officials — It is never permissible to hire or engage a government official, or his or her immediate family members, to improperly influence the official, or in exchange for any improper favor or benefit. Note that before hiring a government official (or relative thereof) Company associates must first receive legal approval from the Company's General Counsel.

Political Contributions — It is never permissible to provide a political contribution to improperly influence a government official, or in exchange for any improper favor or benefit. For additional information and consultation on political contributions, employees should contact the Company's General Counsel.

Discipline and Prosecution

Any person found violating this Policy and its accompanying Manual may be subject to employee discipline, up to and including termination. In addition, any person who violates the FCPA, the U.K. Bribery Act or local anti-bribery laws may find themselves subject to criminal prosecution by U.S., U.K. or local authorities.

Please see ANTI-BRIBERY PROGRAM COMPLIANCE MANUAL for more information.

Anti-Corruption Policy

Euronet is known for its honesty and conscientious behavior. It is the foundation of our business and the reason for our success. Euronet should adhere to all relevant rules and regulations when conducting business. Every relationship our business has is greatly impacted by our reputation. It affects how investors view us as an investment, how consumers view our services, and how our staff, consultants, and agents interact with one another. Every one of us must abide by the Euronet Anti-Corruption, Economic Sanctions, and Export Controls Policy while conducting business globally and with consideration for local situations.

Enforcement

Regardless of where we work, this policy is applicable to all of us, including directors, officers, employees,consultants, and agents. It is our collective responsibility to uphold Euronet's reputation and to act morally.

All individuals connected to Euronet are required to comprehend and abide by all relevant laws and regulations in the nations where we conduct business, in addition to this policy and any other Euronet rules and guidelines.

In addition to economic sanctions on transactions with sanctioned nations and individuals, the United States and other nations in which Euronet conducts business, including the UK and member states of the European Union,maintain controls on the export, reexport, or transfer of goods, software, technology, and services (collectively,"export controls"). Serious civil and criminal fines, denial of participation in government contracts, and other administrative and civil penalties are all possible outcomes of breaking these laws. It is imperative that everyone connected to Euronet take reasonable steps to prevent potential violations when circumstances imply that a customer or a transaction might be in violation of these laws.

The Foreign Corrupt Practices Act ("FCPA") of the United States, which went into effect in 1977, prohibits offering or supplying cash or anything of value to representatives of foreign political parties or governments with the aim to win over or hold onto business. Euronet, like all of its employees, is subject to this law. Canada established the Foreign Public Corruption Act in 1999. This act prohibits offering or providing any form of favor or benefit to a foreign official for the foreign official's advantage. The UK approved the UK Bribery Act in 2011,which prohibits the bribery of public officials and significantly increased the implementation of anti-corruption laws government representatives, including both direct and indirect commercial bribery.

Please contact the General Counsel right away if you have any queries about adhering to this policy. It is our collective responsibility to uphold Euronet's reputation and to be in compliance with these laws and regulations.

Harassment & Sexual Harassment Policy

Euronet is a harassment- and discrimination-free environment.

Euronet does not accept illegal harassment or discrimination in any form, whether verbal, physical, or visual. The HR team at Euronet is dedicated to looking into any instances of harassment or discrimination, including sexual harassment as that term is defined in this policy.

Bullying is one of the numerous forms of discrimination and harassment that can happen based on a range of qualities, in a range of settings, and towards one or more individuals. You do not have to be the target of harassment;it can also happen if you see someone else being harassed. When someone is subjected to unwelcome behavior that violates their dignity or creates an environment that is threatening, hostile, demeaning, embarrassing, or insulting to them, it is considered harassment.

Regarding race, religion, creed, color, national origin, ancestry, physical or mental disability, medical condition,genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, military status, veteran status, or any other basis protected by federal, state, or local law, ordinance, or regulation, Euronet forbids discrimination or harassment of any employee. This anti-discrimination and harassment policy is applicable to all individuals involved in the operation of Euronet and forbids managers, supervisors, coworkers, and outside parties from engaging in unlawful discrimination or harassment against Euronet employees.

To ensure that we all follow this policy, it is crucial that you understand it. We anticipate that you will notify Euronet of any harassment or discrimination, as Euronet may be held accountable even in cases where management is unaware of the harassment or discrimination. The harasser may also be held personally accountable for any damages, as may any management representative who was aware of the harassment and approved or tolerated it.

At Euronet, sexual harassment is not condoned nor allowed. Unwelcome sexual advances, requests for sexual favors,and other verbal, visual, or bodily acts that are sexual in nature—including sexual assault—are all considered forms of sexual harassment. This term covers a wide range of objectionable behavior, including harassment of a person of the same sex by another person on the basis of their gender. A partial list of actions that qualify as harassment is as follows:·

- Unwanted sexual advances or propositions.
- Offering employment benefits in exchange for sexual favors.
- Making or threatening reprisals after a negative response to sexual advances.
- Visual conduct: leering, making sexual gestures, displaying sexually suggestive objects or pictures, cartoons, or posters.
- Verbal conduct: making or using derogatory comments, epithets, slurs, and jokes.
- Verbal abuse of a sexual nature, graphic verbal commentaries about an individual's body, sexually degrading words used to describe an individual, suggestive or obscene letters, notes, or invitations.
- Physical conduct: touching, assault, impeding or blocking movements.

No matter how severe the harassment is, you must report it right away to your supervisor or the HR team at Euronet if you witness harassment or experience it firsthand from a coworker, manager, or outside vendor. It is your responsibility to report someone whose actions make you feel uncomfortable or insulted, even if they are not meant for you. Please include the name(s) of any witnesses, the specifics of the incident(s), and the circumstances surrounding the harassment. Any occurrence of harassment or discrimination must be reported by all supervisors to the Ethics & Conduct team so that it can be investigated. Euronet will investigate the claims in-depth, promptly, and impartially starting right now.

If it is found that harassing behavior has taken place, appropriate corrective measures in line with the seriousness of the infraction shall be implemented. Any worker that Euronet finds to have engaged in harassment or discrimination will face appropriate disciplinary action, which may include termination. The investigation's findings will be shared with all parties involved by a Euronet representative. Euronet will not take any negative action against the employee who reported the harassment or discrimination for making a good faith complaint, and Euronet will not allow or condone employee retaliation. Additionally, Euronet will not accept or condone retaliation against any worker who takes part in a harassment or discrimination investigation.

It is prohibited to use this policy to file harmful or baseless complaints against managers or staff members. If a complaint is brought in bad faith, the individual making it will face disciplinary action, which may include termination.

Euronet's legal obligations to ensure resolution will apply to all complaints and processes including allegations of discrimination or harassment, and all information will be kept confidential to the greatest extent feasible. Euronet will always try to keep the identities of all parties concerned private, apart from what is required to conduct a complete investigation.

Diversity, Equity & Inclusion Policy

Euronet is committed to advancing the diversity of our workforce across all geographies and levels of management, inclusive of ethnicity, and gender diversity.

Euronet adheres to the Equal Opportunity Employer (EOE) guidelines specifically prohibiting from considering race, ethnicity, or gender in its hiring and promotion activities. These anti- discrimination policies are also applicable to the selection of members of our Board of Directors. Additionally, our Board believes that its membership should continue to reflect a diversity of gender, ethnicity, age, sexual orientation, and gender identity.

ADA & ADAAA

Americans with Disabilities Act (ADA) and American with Disabilities Act Amendments Act (ADAAA) are U.S. federal laws that prohibit employers with 15 or more employees from discriminating against applicants and individuals with disabilities and that, when needed, provide reasonable accommodations to applicants and employees who are qualified for a job, with or without reasonable accommodations, so that they may perform the essential job duties of the position.

It is the policy of Euronet to comply with global and national laws concerning the employment of persons with disabilities and to act in accordance with regulations and guidance issued by the Equal Employment Opportunity Commission (EEOC). Furthermore, our policy is not to discriminate against qualified individuals with disabilities regarding application procedures, hiring, advancement, discharge, compensation, training or other terms, conditions,and privileges of employment.

The company will reasonably accommodate qualified individuals with a disability so that they can perform the essential functions of a job unless doing so causes a direct threat to these individuals or others in the workplace and the threat cannot be eliminated by reasonable accommodation and/or if the accommodation creates an undue hardship to the company.

Genetic Nondiscrimination

The Genetic Information Nondiscrimination Act (GINA) of 2008 is designed to prohibit the use of genetic Information in health insurance and employment. The company does not conduct any genetic testing on any applicant or employee under any circumstance and does not discriminate against any applicant or employee because of the individual's genetic information (including information from genetic tests, the genetic tests of family members, the manifestation of a disease or disorder in a family member, family medical history, or information about any employee's, applicants,or family member's request for or receipt of genetic services). Nor does the company request, require, purchase, or intentionally acquire any genetic information.

To the extent the company receives information about an applicant's or employee's family medical history or other genetic information inadvertently (e.g., in the administration of a leave request or accommodation request), that information will not be used except as required for any legitimate purpose (e.g., to consider an employee's leave request relating to a family member's medical condition), and will be treated and maintained as a confidential medical record and will not be disclosed except as allowed or required by applicable law.

Testing for drug or alcohol use is not considered "genetic testing," and may be required by the company in appropriate circumstances. Consistent with the general prohibition against genetic testing of any applicant or employee, any specimen(s) gathered for drug and alcohol testing will not be tested for any genetic information.

We will not retaliate against any individual because the individual honestly and in good faith makes a complaint of discrimination based on genetic information.

Energy Transition Plan

Recently businesses were under increased pressure to be genuine, trustworthy, truthful, and transparent in the current climate. Being the one of the top providers in the world for financial, regulatory, and environmental, social, and governance ("ESG") reporting, these expectations are the core of Euronet's philosophy.

Euronet is dedicated to providing our customers with unwavering services and goods while lessening our environmental effect. We are currently assessing and striving to lower the environmental impact of our own operations and reduce our carbon footprint both locally and worldwide, in addition to supporting the ESG-focused activities of our customers.

Prospective Remarks / Exclusions

This Environmental and Climate Change Statement contains certain statements that are covered by the safe harbor established by Sections 21E of the Securities Exchange Act of 1934, as amended, and 27A of the Securities Act of 1933. These statements are therefore considered "forward-looking statements." Words like "may," "will," "could," "would," "should," "expect," "plan," "anticipate," "believe," "target," or other words of a similar kind can occasionally be used to identify aspirational, future events or condition statements. This paper may contain forward-looking statements about our climate-related programs, aims, plans, aspirations, commitments, and strategies, among other things.

By definition, they are predicated on present plans, projections, and expectations that are rife with assumptions, risks,and uncertainties. Therefore, there are no promises or assurances that they will materialize or be carried out effectively. Euronet disclaims any intention or duty to update or alter any forward-looking statements, whether as a result of new information, future events, or otherwise. Any forward-looking statements are given only as of the date hereof, and unless otherwise required under applicable legislation.

The term "material" or "materiality" used in this Environmental and Climate Change Statement and in all other Environmental documents refers to Euronet's evaluation of ESG priorities to represent the ESG concerns that are significant to us and our stakeholders. When used in this context, these phrases should not be confused with the terms "material" and "materiality," which are defined differently by securities legislation and should not be used in relation to financial statements and reporting.

Anti-Slavery & Human Trafficking Policy

Modern slavery is a crime and a violation of fundamental human rights. It takes many forms, including slavery, servitude, forced and compulsory labor, and human trafficking, all of which involve the deprivation of a person's liberty by another in order to exploit them for personal or commercial gain.

Euronet Worldwide, Inc. takes a zero-tolerance approach to modern slavery, and we are committed to acting ethically and with integrity in all of our business dealings and relationships, as well as implementing and enforcing effective systems and controls to ensure modern slavery does not exist anywhere in our own business or in any of our supply chains.

We are also committed to ensuring transparency in our own operations and in our approach to combating modern slavery throughout our supply chains, in accordance with our disclosure obligations under the Modern Slavery Act. We expect the same high standards from all of our business partners, we will continue to include specific prohibitions against the use of forced, compulsory, or trafficked labor, as well as anyone held in slavery or servitude, whether adults or children, in our contracting processes, and we expect our business partners to hold their own business partners to the same high standards.

This policy applies to all individuals who work for us or on our behalf in any capacity, including employees at all levels,directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants,third-party representatives, and business partners.

This policy is not part of any employee's employment contract, and we reserve the right to change it at any time.

Policy Responsibilities

This policy sets forth our legal and ethical commitments, as well as that all people under our control abide by it. Euronet Worldwide, Inc. is in charge of implementing this policy on a daily basis, monitoring its usage and effectiveness, dealing with any questions about it, and reviewing internal control systems and processes to ensure they are successful in combating modern slavery.

Management at all levels is responsible for ensuring that people reporting to them understand and comply with this policy, as well as that they get proper and ongoing training on it and the subject of modern slavery in supply chains. Feedback and suggestions for the improvement of this policy are welcomed.

Any comments, suggestions or queries are encouraged and should be addressed to HR Department.

Policy Compliance

You must read, understand, and enforce this policy. The prevention, identification, and reporting of modern slavery in any element of our company or supply chains is the duty of everyone who works for us or is under our authority. Refrain from engaging in any action that might lead to or imply a violation of this policy.

If you have reason to believe that a conflict with this policy has occurred, is happening, or may occur in the future, please contact your line manager or a business director as soon as possible. You are urged to express concerns about any issue or suspicion of modern slavery in any aspect of our business or any business partners tier's supply chain as soon as possible.

Note that where appropriate, and with the welfare and safety of local workers as a priority, we will give support and guidance to our business partners to help them address coercive, abusive, and exploitative work practices in their own business and supply chains.

If you have any doubts about whether a specific act, the treatment of employees in general, or their working circumstances inside any tier of our supply chains represents any of the numerous types of modern slavery, please contact your line manager or a company director.

We want to promote transparency and will assist anybody who expresses serious concerns in good faith under this policy, even if those worries turn out to be incorrect. We are dedicated to ensuring that no one experiences any adverse treatment as a result of reporting in good faith their concern that modern slavery in any form is or may be occurring in any section of our own business or in any of our supplier networks.

Dismissal, disciplinary action, threats, or other unfavorable treatment as a result of voicing a concern is considered detrimental treatment. If you suspect you have been subjected to such treatment, you should immediately notify your line manager. If the problem is not resolved, and you are an employee, you should file a formal complaint.

Communication & Awareness

Training on this policy, as well as the threat our company faces from modern slavery in its supply chains, is part of the induction process for all new employees, and updates will be offered through established channels of communication between the company and you.

Our zero-tolerance stance to modern slavery must be conveyed to all suppliers, contractors, and business partners from the beginning of our commercial engagement with them and reinforced as needed subsequently.

Policy Breaches

Any employee who violates this policy may face disciplinary action, which might result in dismissal for misconduct. If other persons or organisations working on our behalf violate this policy, we reserve the right to terminate our relationship with them with immediate effect.

Health & Safety Policy

It is the joint obligation of Euronet and all of its workers to create and maintain a safe work environment. Euronet makes an effort to guarantee a secure workplace and adherence to all occupational health and safety regulations that are relevant for each jurisdiction in which Euronet conducts business.

You must follow safety procedures and use caution when performing any task at work. You have an obligation to notify your manager or another management person right away if you see something unsafe. Euronet will investigate the situation and, if necessary, take appropriate action.

Euronet is dedicated to giving staff members a space where they may come forward with concerns about unsafe working circumstances of any kind.

Notify management right away if you ever come across a strange person at your workspace. When leaving personal belongings unattended, especially in or on desks overnight, proceed with caution.

Weapons are not permitted in any way on Euronet property.

Introduction

Euronet Workplace Health and Safety Policy, hereinafter the "policy," outlines the duties and obligations of various company stakeholders regarding a safe working environment.

This Workplace Health and Safety Policy is put in place to ensure the safety of all the employees, contractors, and any authorized visitors on the company premises. The company fully accepts any rules and regulations enacted by the legislature. The company's Chief Executive will conduct an annual follow-up on the policy and report on its effectiveness.

Obligations

The company is fully committed to ensuring a safe and healthy environment on its premises. To do so, the company will take all necessary and possible measures to remove any hazards or risks. Further, the company will ensure that all its operations are carried out safely and do not pose any danger to either the workers who are authorized visitors.

Company Responsibilities

The company will ensure the following to provide a safe and healthy environment:

- Ensure a safe work environment by putting signs like escape routes clear at all times.
- All its equipment's are up to date.
- Provision of safety facilities for workers
- The company will provide periodic training and safety drills.
- Provide information and instruction regarding health and safety.
- Listen to employees' complaints about health and safety and co-operate with them.

Employee Responsibilities

The employees have the following responsibilities:

- The employee, to their maximum capacity, will adhere to the safety practices.
- They will ensure reasonable care of themselves and co-workers.
- Participate in training and safety drills.
- Wear protective equipment while working.
- Report any safety issue immediately to the company.
- Read and comply with the instructions provided on the company premises.

General

- It is everyone's responsibility to keep exits, hallways, and corridors clear at all times.
- Vehicles should be parked at the designated place and must not be parked at random places.
- Any suspected hazard or violation of safety measures must be reported immediately to the health and safety officer.

Data Protection & Privacy Policy

Introduction

Euronet Worldwide, Inc. ("Euronet", "Company" or "we") is a world leader in electronic payment services and transaction processing solutions and operates globally. In providing our services, we store and transmit a large amount of personal data. We understand that protecting the rights and privacy of each and every individual whose personal data we handle is fundamental to trust in our business relationships. We have, therefore, committed to ensuring a high level of data protection and data security across our business.

This Data protection & Privacy Policy sets out how we will process personal data and applies to every Euronet employee, contractors, suppliers or any other member of staff. We expect all employees, and other members of staff, to familiarize themselves with this policy, and to act in accordance with it in the performance of their duties and responsibilities. Failure to comply with this policy may subject Euronet, its employees and staff to civil and/or criminal liability. Employees or any other members of staff who fail to comply with this policy will be subject to disciplinary action up to and including termination of employment.

The effectiveness of this policy depends largely on employees and all other members of staff. If you feel that you or someone else may have violated this policy, you should report the incident immediately to your supervisor. If you are not comfortable bringing the matter up with your immediate supervisor, or do not believe the supervisor has dealt with the matter properly, you should contact the European Data Protection Officer if you are based in Europe or the Global Data Protection Officer or legal department if based outside Europe.

Scope

Euronet is committed to international compliance with data protection laws. This Data Protection & Privacy Policy ensures an adequate level of data protection prescribed by applicable laws, including the EU General Data Protection Regulation ("GDPR") and applicable laws for cross-border data transmission, including in countries that do not yet have adequate data protection laws.

This Data Protection & Privacy Policy applies to all companies within the Euronet Worldwide, Inc. group of companies and their employees and other staff members (the "Euronet Group"). "Dependent" in this instance means that Euronet Worldwide, Inc. may enforce the adoption of this Data Protection Policy directly or indirectly, on the basis of voting majority, majority management representation, or by agreement. The Data Protection Policy extends to all processing of personal data.

Definitions

"Personal data" means any information relating to a living individual (known as a **"data subject"**) who can be identified from that information (either directly or indirectly when combined with other information in the Company's possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behavior. Personal data includes sensitive personal data.

The Company will control personal data relating to employees, and other members of staff, as well as its customers, suppliers or other third parties as well as their employees and staff members. The protections under this Data Protection Policy apply equally to all data subjects, whether or not employees of the Company.

This Data Protection Policy applies to any "processing" of personal data by the Company or by a third party on its behalf. The term "processing" may include the Company obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including organizing, altering, retrieving, consulting, using, disclosing or destroying the information or data. Processing also includes sharing personal data with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries.

Principles for Processing of Personal Data

Personal data held must be:

- Processed fairly, lawfully and in a transparent manner.
- Obtained and processed only for specified, explicit and legitimate purposes and not in a way that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary for the purpose it is processed.
- Accurate and, where necessary, kept up to date.
- Kept no longer than is necessary for the purpose it is processed.
- Processed in a manner that ensures appropriate security, using all appropriate technical or organizational measures.
- Processed in line with data subjects' rights; and
- For personal data of Data Subjects based in Europe, not transferred to a country outside the European Economic Area ("EEA") unless there is an adequate level of data protection in that country or unless the transfer of personal data is covered by another legal means for transferring such personal data.

Purposes for Which Personal Data May Be Processed

Personal data will be processed in accordance with applicable laws where the data subject has given his/her consent for one or more specific purposes, or where the processing of personal data is necessary for:

- The performance of a contract to which the data subject is a party.
- Compliance with a legal obligation.
- The protection of the vital interests of the data subject or another natural person; or
- The processing is necessary for one or more specific purpose(s) in the legitimate business interests of the Company; or
- Any other legal basis under applicable laws.

With regard to the processing of personal data relating to the Company's employees or other members of staff, we process such personal data based on the legitimate interest of the Company, which include, but are not limited to:

- Recruitment, Pre-employment screening, promotion, training, redeployment and/or career development.
- Administration and payment of wages.
- Calculation of certain benefits including pensions.
- Disciplinary or performance management purposes.
- Monitoring of employees.
- Providing security at company locations.
- Recording of communication with you and your representatives.
- Compliance with legislation.
- Provision of references to financial institutions, to facilitate entry onto educational courses and/or to assist future potential employers.
- Staffing levels and career planning; and
- In order to protect our rights, property or safety of our employees, customers or others.

The Company considers that the following personal data falls within the purposes set out above:

- Personal details including name, address, age, status and qualifications. Where specific monitoring systems are in place, ethnic origin and nationality will also be deemed as relevant.
- References and CVs.
- Emergency contact details.
- Notes on discussions between management and you.
- Appraisals and documents relating to grievance, discipline, promotion, demotion or termination of employment.
- Training records.
- Salary, benefits and bank/building society details; and
- Absence and sickness information.

Employees or potential employees, and other staff members, may be advised by the Company of the personal data which has been obtained or retained, its source, and the purposes for which the personal data may be used or to whom it will be disclosed.

The Company will regularly review the nature of the information being collected and held as required by applicable law to ensure there is a sound business reason requiring the information to be retained.

Sensitive Personal Data

The Company may obtain and process sensitive personal data of employees in connection with your employment to meet applicable legal obligations. Sensitive personal data (or "special categories of personal data") includes information relating to the following matters:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Physical or mental health or condition.
- Sex life or sexual orientation; or
- Commission or alleged commission of any offence.

To hold sensitive personal data, the Company must satisfy an additional sensitive data condition. The processing of such special categories of personal data is necessary to enable the Company to meet its legal obligations (e.g. to ensure health and safety or avoid unlawful discrimination).

Responsibility for the Processing of Personal Data

The Company has appointed a Data Protection Officer in Europe and other Global Data Protection compliance resources globally that are responsible for ensuring all personal data is controlled in compliance with this Data Protection Policy.

Employees, or other members of staff, who have access to personal data must comply with this Policy and adhere to the procedures laid down by the Company. Failure to comply with the Policy and procedures may result in disciplinary action up to and including summary dismissal.

Use of Personal Data

To ensure compliance with this Data Protection Policy and in the interests of privacy, employee/customer confidence and good employee/customer relations, the disclosure and use of information held by the Company is governed by the following conditions:

- Personal data may only be processed for one or more of the purposes specified in this policy or as permissible under applicable laws.
- Company documents may only be used in accordance with the statement within each document stating its intended use; and
- Provided that the identification of individual data subjects is not disclosed, aggregate or statistical information may be used to respond to any legitimate internal or external requests for data (e.g. surveys, staffing level figures).

Disclosure of Personal Data

Personal data may only be disclosed outside the Company to third parties:

- In the event that the Company sells or buys any business or assets, in which case the Company may disclose personal data to the prospective seller or buyer of such business or assets.
- If the Company or substantially all of its assets are acquired by a third party, in which case personal data will be one of the transferred assets.
- With the data subject's written consent.
- Where disclosure is required by law.
- Where there is immediate danger to the data subject's health; or
- On the basis of a specific purpose in the legitimate business interests of the Company as set out in this policy or as otherwise notified to the data subject.

Transfer of Personal Data

Transmission of personal data to recipients outside or inside the Euronet Group is subject to the authorization requirements for processing personal data under this Data Protection Policy. The data recipient must be required to use the data only for the defined purposes.

If personal data is transferred from a Group company with its registered office in the EEA to a Group company outside of the EEA, the transfer must be compliant with this Data Protection & Privacy Policy. The Group company based in the EEA that transmits the personal data shall be held liable to any European data subject for any violations of this Data Protection Policy committed by the Group company located in a third country.

If personal data is transferred from a Group company with its registered office in the EEA to a third party outside of the EEA, one of the following conditions must apply:

- The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The Company and the recipient have provided appropriate safeguards to ensure that the personal data is protected and that effective legal remedies are available, i.e. standard data protection clauses adopted by the European Commission or other relevant authority.
- The data subject has given his/her explicit consent.
- The transfer is necessary for the performance of a contract between the data subject and the Company

If you have any questions about the transfer of personal data from the EEA in accordance with this Data Protection Policy or would like further information about our compliance with the obligations, please contact the Data Protection Officer.

Accuracy of Personal Data

The Company will review personal data regularly to ensure that it is accurate, relevant and, where necessary, up to date.

In order to ensure the Company's files are accurate and up to date, and so that the Company is able to contact the employee or, in the case of an emergency, another designated person, employees must notify the Company as soon as possible of any change in their personal details (e.g. change of name, address, telephone, loss of driving license where relevant, next of kin details, etc.).

Timely Processing

The Company will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. The Company will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required in line with the **"Document & Data Retention Policy"**.

European Data Subject Rights

Under the GDPR, in certain circumstances data subjects, including employees and other staff members of the Company, have the right to:

- Request access to any data held about him/her ("Subject Access Request").

- Ask to have inaccurate data amended.
- Request personal data held about him/her be deleted provided the data is not required by the Company to perform a contract or defend a legal claim;
- Prevent or restrict processing of personal data which is no longer required or if accuracy of data is contested and data subject opposes erasure; and
- Request transfer of appropriate personal data to a third party where this is technically feasible; and
- Object to automated decision making that could affect a data subject's rights.

In addition, where the data subject believes that the Company has not complied with its obligations under this policy or the GDPR, he/she has the right to make a complaint to the relevant supervisory authority.

If you are based in Europe and would like to exercise one or more of your data subject rights listed above, please contact European Data Protection Officer via email, DPO@euronetworldwide.com, or post, Data Protection Officer, Edificio Amura, C/ Cantabria nº2, 2-planta, 28108 Alcobendas, Madrid, Spain.

If any employee or other staff member receives a request to exercise one or more of the above data subject rights from any data subject (including Company employees, staff members, customers, suppliers or their employees or staff members), the request must be handled in accordance with the "Data Subject Rights Request Policy".

The Company aims to respond to Subject Access Requests without undue delay and in any event within one month of the receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of requests. The Company may charge a reasonable fee or refuse to act on request(s), where the request(s) are manifestly unfounded, frivolous, vexatious, excessive jeopardize the privacy of others, or for which access is not otherwise required by local law.

Data Security

The Company will process all personal data it holds in accordance with our **"Information Security Policy"**.

The Company will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if the data processor agrees to comply with those procedures and policies, or if the data processor puts in place adequate measures.

The Company will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorized to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorized users should be able to access the data if they need it for authorized purposes.

Any personal data breach or accidental loss must be immediately reported to the local head of IT and designated security officer. Any such incident will be dealt with by the Company in line with our "Global Incident Response Plan".

Changes to this Policy

The Company reserves the right to change this policy at any time. Where appropriate, the Company will notify data subjects of those changes by mail or email.

Insider Trading & Confidentiality Policy

Euronet Worldwide, Inc. has listed its shares on The Nasdaq Global Select Market in the United States. As a result, we have legal and ethical responsibilities to establish rigorous internal procedures regarding the flow of information within the Company and from the Company to the public. U.S. federal securities laws prohibit the purchase or sale of securities by directors, officers, employees, and others who are aware of material non-public information about a company, as well as the disclosure by such persons of material non-public information to others who may trade in that company's securities. Public companies are also subject to liability if they fail to take reasonable steps to prevent insider trading by their personnel. In other words, the Company is required to take steps to ensure that directors, officers, employees, and others do not directly or indirectly trade on "inside information."

The Board of Directors has adopted the following Policy which applies to all directors, officers, employees, contractors, consultants, and advisers of the Company. For purposes of this Policy, the "Company" includes Euronet Worldwide, Inc. and all of its subsidiaries and affiliated companies. It is your obligation to understand and comply with this Policy.

Should you have any questions regarding this Policy, please contact the Company's General Counsel.

Persons Subject to this Policy

Because you are a director, officer, employee, contractor, consultant or adviser of the Company, this Policy applies to:

- you,
- your family members who reside with you,
- anyone else who lives in your household,
- any family members who do not live in your household but whose transactions in Company securities are directed by you or are subject to your influence or control (such as parents or children who consult with you before they trade in Company securities),
- any entity controlled by you or by any of your related persons listed above, and
- any other person or entity designated by the Company's General Counsel.

You are responsible for the transactions of these other persons and entities and therefore you should make them aware of the need to confer with you before they purchase or sell or otherwise transfer the Company's securities. As used below, "you" means anyone subject to this Policy.

Because of the opportunity to profit from information obtained while serving as a director, officer, employee, contractor, consultant or adviser of the Company, this Policy continues to apply to any director, officer, employee, contractor, consultant or adviser of the Company and their related persons described above for a period of six months after the director, officer, employee, contractor, consultant or adviser terminates his or her employment or affiliation with the Company, unless otherwise determined by the Company's General Counsel. In addition, if such persons are in possession of material non-public information when their employment or affiliation with the Company terminates, they may not purchase or sell or otherwise transfer Company securities prior to the time that such information has become public or is no longer material.

Prohibition Against Trading on or Disclosing Material Non-public Information

If you are aware of material non-public information relating to the Company or you are aware that the Company is in possession of material non-public information (often called "inside information"), you are prohibited from purchasing or selling or otherwise transferring our securities, directly or indirectly, and from disclosing such information to any other persons (including relatives, friends, brokers, investment advisers, etc.). You are subject to liability if you trade at the time you possess material non-public information, without regard to whether your decision to trade was based on that information. As used in this Policy, the term "securities" includes, (i) all securities issued by the Company, including common stock, options, preferred stock, notes, bonds and convertible securities, and (ii) in addition to securities issued by the Company, any put, call, straddle, option, derivative security or group or index of securities issued or created by a third party that relates to or includes Company securities, in each case whether or not publicly traded.

Material Information

Any information, positive or negative, is "material" if a reasonable investor is substantially likely to consider it important in determining whether to purchase, sell or hold our securities. Information is considered to be material if it would be expected to affect the market price of our securities. Information may be material for this purpose even if it would not alone determine the investor's decision.

Examples include:

- a potential business acquisition or disposition,
- Financial projections, forecasts, or budgets,
- Internal information about revenues, earnings or other aspects of financial performance which departs in any way from what the market would expect based upon prior disclosures,
- Change in laws and regulations
- Important business developments,
- The acquisition or loss of, or change in the terms of any contract with, a major supplier or content provider
- Changes in senior management,
- Major events regarding the Company's securities, such as a dividend, stock split or share repurchase
- Actual or threatened major litigation, or the resolution of such litigation, or
- an important transaction.

We emphasize that this list is merely illustrative. In addition to historical information, information which is forward- looking or contingent may be material. If you are unsure whether the information is material, you should consult with the Company's General Counsel before taking any action. When in doubt, information should be presumed to be "material."

Non-Public Information Information may be considered "non-public" if it has not been disseminated in the Company's SEC filings or has not been the subject of a prior widely disseminated Company press release. The fact that information has been disclosed to a few members of the public or appears on the Company's website does not make it public for insider trading purposes. Unless the Company publicly confirms information reported by the news media, analysts or other third-party sources, such information may still be considered non-public. You should be aware that it is the Company's policy not to comment on such information.

Once all material information is publicly disseminated, trading can occur after a lapse of two full trading days, unless the Company determines that a shorter period is sufficient. Therefore, if an announcement is made before the commencement of trading on a Monday, a covered person may trade in the Company's stock starting on the Wednesday of that week, because two full trading days would have elapsed by then (all of Monday and Tuesday). If the announcement is made on Monday after trading begins, covered persons may not trade in the Company's stock until Thursday. Release of some material information does not allow insiders to trade if other material information remains undisclosed.

Please consult the General Counsel of the Company, if you are uncertain whether the information has been made public and when trading may commence following a public announcement by the Company. When in doubt, information should be presumed to be "non-public" and treated as confidential.

Compliance with Restrictions

The above prohibition against trading on or disclosing inside information generally reflects the requirements of law as well as the Company's Policy. It is impossible to overstate the importance of understanding and complying with the insider trading laws. You need not be an officer or senior executive of the Company to be subject to the insider trading laws. Any employee or other person with access to inside information is subject to prosecution for a violation.

As fully discussed below, a breach of this Policy will subject you to disciplinary action by the Company and probably will constitute a serious legal violation as well. In all cases, the responsibility for determining whether you are in possession of material non-public information and in compliance with this Policy rests with you, and any action on the part of the Company, the General Counsel or any other employee or director pursuant to this Policy (or otherwise) does not in any way constitute legal advice or insulate you from liability under applicable securities laws.

Confidentiality Generally

Serious problems could be caused for the Company by unauthorized disclosure of internal information about the Company (or confidential information about our business partners), whether or not for the purpose of facilitating improper trading in our stock or other securities. You should not discuss internal Company matters or developments with anyone outside of the Company or with co-workers who are not involved in such matters, except as required in the performance of your regular duties on behalf of the Company.

This prohibition on disclosing confidential information applies specifically (but not exclusively) to inquiries about the Company which may be made by the financial press, investment analysts or others in the financial community. It is important that all such communications on behalf of the Company be made only pursuant to the Company's Disclosure Policy. The Company is required under Regulation FD of the U.S. federal securities laws to avoid the selective disclosure of material non-public information. The Company has established procedures for releasing information in a manner that is designed to achieve broad public dissemination of the information. Unless you are expressly authorized to the contrary, if you receive any inquiries of this nature, you should decline comment and refer the inquiry to the Head of Investor Relations or the General Counsel of the Company.

Information About Other Companies. In the course of your employment or affiliation with the Company, you may become aware of material non-public information about other public companies — for example, other companies with which our Company has business dealings. You are prohibited from purchasing or selling or otherwise transferring the securities of any other public company at a time when you are in possession of material non-public information about such company. You are also prohibited from disclosing such information to another person who trades in such a company's stock or other securities.

Tipping

Improper disclosure of material non-public information to another person who trades in the stock or other securities (so-called "tipping") is also a serious legal offense by the tipper and a violation of the terms of this Policy. If you disclose material non-public information about our Company, or material non-public information about any other public company which you acquire in connection with your employment or affiliation with our Company, or if you advise anyone to purchase or sell securities based upon such information, you may be fully responsible legally for the trading of the person receiving the information from you (your "tippee") and even persons who receive the information directly or indirectly from your tippee, whether or not you are aware of any trading by such persons.

Accordingly, in addition to your general obligations to maintain confidentiality of information obtained through your employment or affiliation with the Company and to refrain from trading while in possession of material non-public information, you must take utmost care not to discuss confidential or material non-public information with family members, friends or others who might abuse the information by trading in securities.

Limitation on Certain Trading Activities.

We encourage interested directors, officers, and employees to own our securities as a long-term investment at levels consistent with their individual financial circumstance and risk bearing abilities (since ownership of any security entails risk). However, Company personnel (which shall include directors, officers, and employees of the Company) may not trade in puts, calls or similar options on our stock or sell our stock "short." Company personnel may not purchase financial instruments (including prepaid variable forward contracts, equity swaps, collars, and exchange funds) or otherwise engage in transactions that are designed to or have the effect of hedging or offsetting any decrease in the market value of our securities.

Margin Accounts and Pledges Securities held in a margin account may be sold by the broker without the customer's consent if the customer fails to meet a margin call. Similarly, securities pledged (or hypothecated) as collateral for a loan may be sold in foreclosure if the borrower defaults on the loan. A margin sale or foreclosure sale may occur at a time when the pledgor is aware of material non-public information or otherwise is not permitted to trade in Company securities.

Consequently, you are discouraged from holding Company securities in a margin account or pledging Company securities as collateral for a loan. In addition, persons subject to the Addendum as described below are prohibited from holding Company securities in a margin account and are restricted from pledging Company securities as collateral for a loan as described in the Addendum.

Transactions under Company Stock Plans.

Certain transactions in Company securities relating to Company stock plans are restricted under this Policy:

(a) Stock Option Exercises; Tax Withholding. This Policy's trading restrictions generally do not apply to the exercise of a stock option for cash. However, you may not sell the underlying shares of stock and you may not engage in a cashless exercise of a stock option through a broker (because this entails selling a portion of the underlying stock to cover the costs of exercise) while you possess material, non-public information. This Policy's trading restrictions generally do not apply to the exercise of tax withholding rights pursuant to which you elect to have the Company withhold shares from an award to satisfy tax withholding requirements.

(b) Employee Stock Purchase Plan. This Policy's trading restrictions do not apply to purchases of Company stock in the employee stock purchase plan resulting from your periodic payroll contributions to the plan under an election you made at the time of enrollment in the plan. The trading restrictions do apply to your sales of Company stock purchased under the plan.

(c) 401(k) Plan. This Policy's trading restrictions do not apply to purchases of Company stock in the 401(k)-plan resulting from the periodic contribution of money to the plan by the Company. The trading restrictions do apply, however, to elections you may make under the 401(k) plan (to the extent then permitted under the 401(k) plan) to (a) increase or decrease the percentage of your periodic contributions, if any, that will be allocated to the Company stock fund, (b) make an intra-plan transfer of an existing account balance into or out of the Company stock fund, (c) borrow money against your 401(k) plan account if the loan will cause a sale of some or all of the shares in the Company stock fund, and (d) prepay a plan loan if the pre-payment will result in allocation of loan proceeds to the Company stock fund.

Gifts

The Company may permit bona fide gifts of stock during periods when trading is restricted, as determined by the General Counsel. Whether a gift is bona fide will depend on the circumstances surrounding the gift, such as whether the gift is made to a charity or to a relative or friend of the donor and whether the shares are to be sold immediately thereafter. If you intend to make a gift during periods when trading is restricted, you must review the gift transaction with the General Counsel prior to making the gift.

Consequences of Violation

The Company considers strict compliance with this Policy to be a matter of utmost importance. We would consider any violation of this Policy by any covered person as a threat to our reputation. Violation of this Policy could cause extreme embarrassment and possible legal liability to you and the Company. Violations of the letter or spirit of this Policy will be grounds for disciplinary action by the Company, including immediate dismissal from the Company. Violation of this Policy might expose the violator to severe criminal penalties, including fines of up to $5 million and imprisonment for up to 20 years, or both, and civil penalties to the SEC of up to three times the profit gained, or loss avoided as a result of the violation. In addition, violators may be subject to civil liability to any person injured by the violation. The monetary damages to persons injured may be as much as three times the profit realized or loss avoided by the violator, as well as the attorney's fees of the persons injured.

Additionally, persons or entities who, at the time of the violation, directly or indirectly "controlled" the person who committed the violation are subject to civil penalties of up to the greater of $1 million or three times the profit gained or loss avoided as a result of the controlled person's violation and criminal penalties of up to $25 million.

The potential for such controlling a person's liability is particularly important for the Company, because the Company (and possibly directors and certain officers of the Company) may be considered to "control" Company employees for this purpose. In view of the potential legal exposure faced by the Company, as well as the potential for significant damage to its business and public relations, the Company will insist upon strict compliance with this Policy.

Resolving Doubts

If you have any doubt as to your responsibilities under this Policy, seek clarification and guidance before you act from our General Counsel. Do not try to resolve uncertainties on your own.

Blackout Periods, Pre-Clearance Procedures and Transaction Reporting. To help prevent violations of the applicable securities laws and to avoid even the appearance of trading on the basis of inside information, the Company has adopted an Addendum to this Policy that applies to (i) directors and executive officers of the Company subject to Section 16 of the Securities Exchange Act of 1934, as amended, (ii) persons who report directly to any such executive officer and (iii) other individuals designated from time to time by Euronet Worldwide, Inc. as being subject to the Addendum. If you fall within one of these categories, you must carefully review and comply with the additional requirements of the Addendum. The Company will notify you if you are subject to the Addendum under clause (ii) or (iii) above.

The Addendum generally requires persons covered by it to pre-clear with the Company all transactions in the Company's securities, prohibits such persons from engaging in transactions in the Company's securities during quarterly earnings blackout periods and other blackout periods designated by the Company, permits such persons to adopt trading plans under certain circumstances, and specifies certain transaction reporting requirements of directors and executive officers.

A Caution About Possible Inability to Sell

Although the Company encourages directors, officers, and employees to own our securities as a long-term investment, all personnel must recognize that trading in securities may be prohibited at a particular time because of the existence of material non-public information. Anyone purchasing our securities must consider the inherent risk that the sale of the securities could be prohibited at a time he or she might desire to sell them. The next opportunity to sell might not occur until after an extended period, during which the market price of the securities might decline.

Amended and Restated as of June 16, 2015

This Addendum applies to (i) directors and executive officers of the Company subject to Section 16 of the Securities Exchange Act of 1934, as amended ("Exchange Act"), (ii) persons who report directly to any such executive officer and (iii) other individuals designated from time to time by Euronet Worldwide, Inc. as being subject to this Addendum (collectively, with their family members, members of their households and persons and entities that they control or influence. The Company will notify the persons described in clauses (ii) and (iii) that they are subject to this Addendum.

This Addendum is in addition to and supplements the Company's Policy Relating to Insider Trading and Confidentiality of Information. Terms defined in the Policy shall have the same meanings in this Addendum.

1. Mandatory Pre-clearance Procedures. Covered Persons may not engage in any transaction involving our securities (including without limitation a gift, a loan or pledge, a hedge, a stock plan transaction such as an option exercise, a contribution to a trust, or any other transfer) without first obtaining pre-clearance of the transaction from the General Counsel. A request for preclearance must be submitted to the General Counsel at least two business days in advance of the proposed transaction. The General Counsel will then determine whether the transaction may proceed. The General Counsel may not engage in any transaction involving our securities unless the Chief Executive Officer approves the transaction in accordance with the procedures set forth in this Addendum. Neither the Chief Executive Officer nor the General Counsel is under any obligation to approve a transaction submitted for pre-clearance, and none of the Company, the Chief Executive Officer or the General Counsel will have any liability for any refusal to permit a transaction or for any delay in making or communicating a decision.

2. Blackout Periods. The persons specified below may not engage in any transaction involving our securities during "blackout periods" as described below. Persons subject to these provisions should note that even if a blackout period is not in effect, (a) Covered Persons must comply with the pre-clearance procedures set forth above and (b) at no time may anyone trade in Company securities if such person is aware of material, non-public information about the Company. For example, if the Company issues a quarterly earnings release and a person is aware of other material, non-public information not disclosed in the earnings release, the person may not trade in Company securities.

(a) Quarterly Blackout Periods. The Company's announcement of its quarterly financial results generally has the potential to have a material effect on the market for the Company's securities. Therefore, in order to avoid even the appearance of trading while in possession of material non- public information, with respect to each fiscal quarter of the Company, Covered Persons may not purchase or sell or otherwise transfer the Company's securities during the period beginning

15 days prior to the end of the quarter and ending after the second full business day following the release of the Company's financial results for that quarter. The announcement date of the quarterly results varies but occurs normally toward the end of the month following the end of the fiscal quarter.

(b) Other Blackout Periods. In addition, the Company may impose event specific restricted periods during which Covered Persons who are aware of the event may not purchase or sell or otherwise transfer any securities of the Company. These blackout periods may be imposed as a result of an event, contingency or potential transaction that may be material to the Company. Also, the Company may on occasion issue interim earnings guidance or other potentially material information by means of a press release, Form 8-K or other means designed to achieve widespread dissemination of the information. Transactions are unlikely to be pre-cleared while the Company is in the process of assembling the information to be released and until the information has been released and fully absorbed by the market.

The existence of an event-specific blackout period may not be announced or may be announced only to those who are aware of the transaction or event giving rise to the blackout period. If you are made aware of the existence of an event-specific blackout period, you should not disclose the existence of such blackout period to any other person or purchase or sell or otherwise transfer any Company securities. Individuals who are subject to event specific blackout periods will be contacted when these periods are instituted from time to time. Whether or not you are designated as being subject to an event-specific blackout, you still have the obligation not to trade while aware of material non-public information.

(c) Pension Fund Blackout Periods. Subject to certain exceptions, directors and executive officers of the Company may not purchase, sell or otherwise acquire or transfer any equity security of the Company during any "pension fund blackout period" with respect to such equity security, if the director or executive officer acquired the equity security in connection with his or her service or employment as a director or executive officer. A pension fund blackout period exists whenever 50% or more of the participants in a Company benefit plan are unable to conduct transactions in their Company equity security accounts for more than three consecutive business days. Individuals who are subject to these blackout periods will be contacted by the Company at such times as these blackout periods occur.

(d) Hardship Exceptions. If you have an unexpected and urgent need to sell Company securities in order to generate cash you may, in appropriate circumstances, be permitted to sell Company securities during a quarterly earnings blackout period. Hardship exceptions may be granted only by the General Counsel and must be requested at least two business days in advance of the proposed transaction.

A hardship exception will not be granted in any event if the General Counsel concludes that the Company's financial results for the applicable quarter constitute material non-public information. The General Counsel is under no obligation to approve a hardship exception, and neither the Company nor its officers shall have any liability for any refusal to grant a hardship exception or for any delay in making or communicating a decision. Under no circumstances will a hardship exception be granted during an event-specific blackout period or pension fund blackout period.

3. Exception for Approved Rule 10b5-1 Trading Plans. Trades by Covered Persons in the Company's securities that are executed pursuant to a Rule 10b5-1 trading plan are not subject to the prohibition on trading while in possession of material non- public information contained in the Policy Relating to Insider Trading and Confidentiality of Information or the restrictions set forth above relating to pre-clearance procedures and blackout periods. A Rule 10b5-1 trading plan is a trading plan adopted pursuant to Rule 10b5- 1 ("Rule 10b5-1") promulgated under the Exchange Act. Notwithstanding any approval of a Rule 10b5-1 trading plan, the Company and its officers assume no liability with respect to any transaction made pursuant to the plan. Rule 10b5-1 trading plans are subject to the following restrictions and limitations:

- The Rule 10b5-1 trading plan must be in writing and approved in advance by the General Counsel of the Company.
- The Rule 10b5-1 trading plan must comply with and be adopted in accordance with the provisions of Rule 10b5-1.
- The Rule 10b5-1 trading plan generally may not be adopted during a blackout period or when a Covered Person is in possession of material non- public information.
- The Rule 10b5-1 trading plan must be entered into in good faith and not as part of a plan or scheme to evade the prohibitions of Rule 10b5-1.
- A Covered Person may not amend or terminate his or her Rule 10b5-1 trading plan without the prior approval of the General Counsel.
- A Covered Person may not separately enter into a corresponding or hedging transaction or position with respect to the securities traded pursuant to the Rule 10b5-1 trading plan.
- A Covered Person or his or her broker must inform the General Counsel of each transaction under the Rule 10b5-1 trading plan so that the Company may monitor compliance with the filing obligations of Section 16 of the Exchange Act and Rule 144 of the Securities Act of 1933, as amended.
- The Rule 10b5-1 trading plan must comply with and be adopted in accordance with the such other requirements as may be directed by the General Counsel, which may include without limitation the imposition of a cooling off period between the adoption or amendment of the Rule 10b5-1 trading plan and the first transaction under the Rule 10b5- 1 trading plan or between the termination of a Rule 10b5-1 trading plan and adoption of a new Rule 10b5-1 trading plan.

4. Margin Accounts and Pledges. Covered Persons are prohibited from holding Company securities in a margin account or pledging Company securities as collateral for a loan. An exception to this prohibition may be granted where a Covered Person wishes to pledge Company securities as collateral for a loan (not including margin debt) and clearly demonstrates the financial capacity to repay the loan without resort to the pledged securities. If a Covered Person wishes to pledge Company securities as collateral for a loan, the Covered Person must submit a request for approval to the General Counsel prior to the proposed execution of documents evidencing the proposed pledge.

5. Accelerated Filing of Reports for Persons Subject to Section 16 of the Exchange Act. Directors and executive officers of the Company subject to Section 16 of the Exchange Act ("Section 16 Insiders") must file beneficial ownership reports regarding their ownership of and transactions in Company securities pursuant to Section l6(a) of the Exchange Act and are subject to disgorgement of "short-swing" profits pursuant to Section l6(b) of the Exchange Act. Under Section 16 of the Exchange Act, the due dates for beneficial ownership reports on Form 4 of Section 16 Insiders are as early as the second business day following a transaction that affects a change in the ownership of our securities.

Given the short time frame for Section 16 Insiders to file their Form 4's, it is critically important that Section 16 Insiders comply with the procedures in this Addendum to ensure compliance with the accelerated reporting requirements. These procedures will help prevent inadvertent violations of the federal securities laws, will help avoid the appearance of insider trading and will prevent potentially embarrassing proxy disclosures. You will be notified if you are a Section 16 Insider. In connection with sale transactions, in many instances you must also file a Form 144 Notice with the SEC under Rule 144 at the time the sale order is placed.

To ensure compliance with the accelerated reporting requirements of Section 16 and to help prevent in advance any inadvertent violations of the federal securities laws, and to avoid even the appearance of trading on inside information, we have implemented the following procedures:

- Mandatory Pre-clearance Procedures. All Section 16 Insiders must comply with the mandatory pre-clearance procedures set forth above.
- Immediate Notification. All Section 16 Insiders must report to the General Counsel any transaction no later than the day in which it has occurred.
- Power of Attorney. In order to enable the Company to prepare and file the Forms 4 on a timely basis, it is imperative that you sign and return the Power of Attorney provided to you by the General Counsel.
- Certifications. All Section 16 Insiders must certify their understanding of, and intent to comply with, the procedures set forth herein.
- Company Assistance. Any person who has a question about these procedures or its application to any proposed transaction may obtain additional guidance from the General Counsel.
- Periodic Preventive E-mail Alerts/Reminders. Because the risk of inadvertent Form 4 filing violations is so high and because of heightened public scrutiny, we will continue our practice of sending you periodic preventive Reminders and Alerts during the course of the year.

Not withstanding the Company's willingness to assist you with your filings, please remember that the reporting obligation is yours.

Social Media Policy

Purpose

Euronet Worldwide, Inc. ("Euronet," "we" or the "Company") recognizes that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media. However, employees' use of social media can (i) pose risks to Euronet's confidential and proprietary information, reputation, and brands, (ii) expose Euronet to discrimination and harassment claims, and (iii) jeopardize the Company's compliance with business rules, securities laws, and other applicable laws.

To minimize these business and legal risks, to avoid loss of productivity and distraction from employees' job performance and to ensure that the Company's IT resources and communications systems are used appropriately as explained below, we expect our employees to adhere to the following guidelines and rules regarding use of social media. All references to "employees" herein shall include contractors and consultants.

Compliance with Related Policies and Agreements

All of our other policies that might apply to the use of social media remain in full force and effect, including, in particular, the **Code of Conduct**. Employees should always adhere to such policies when using social media.

Social media should never be used in a way that violates any other Euronet policies or employee obligations. If your social media activity would violate any of Euronet's policies in another forum, it will also violate them in an online forum.

For example, employees are prohibited from using social media to:

- Violate Euronet's IT resources and communications systems policies.
- Violate Euronet's confidentiality and proprietary rights policies.
- Circumvent Euronet's ethics and standards of conduct policies, including the Code of Conduct.
- Engage in unlawful harassment.
- Circumvent policies prohibiting unlawful discrimination against current employees or applicants for employment.
- Violate Euronet's privacy policies (for example, never access private password protected sites of co-workers or other Euronet stakeholders without permission).
- Violate any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by creating an artificial "buzz" around our business, products, or stock).

Employees who violate Euronet policies may be subject to discipline, up to and including termination of employment.

Personal Use of Social Media

We recognize that employees might work long hours and occasionally may desire to use social media for personal activities at the office or by means of the Company's computers, networks and other IT resources and communications systems. We authorize such infrequent and occasional use so long as it does not (i) involve vulgar, obscene, threatening, intimidating, or harassing content, (ii) violate any other Euronet policies or employee obligations, or (iii) interfere with your employment responsibilities or productivity. Circulating or posting commercials, personal, religious, or political solicitations, chain letters, spam, or promotion of outside organizations unrelated to Company business are also prohibited.

No Expectation of Privacy All contents of Euronet's IT resources and communications systems are the property of the Company. Therefore, unless otherwise expressly provided by local law, employees should have no expectation of privacy whatsoever in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on the Company's electronic information and communications systems.

You are expressly advised that in order to prevent misuse, and subject to the application of any local laws which may limit our rights to do so, Euronet reserves the right to monitor, intercept and review, without further notice, every employee's activities using the Company's IT resources and communications systems, including but not limited to social media postings and activities, and you consent to such monitoring by your acknowledgment of this policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving, and printing of transactions, messages, communications, postings, logins, recordings, and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

We also may store copies of such data or communications for a period of time after they are created and may delete such copies from time to time without notice.

Do not use the Company's IT resources and communications systems for any matter that you desire to be kept private or confidential from the Company.

Business Use of Social Media

If you are required to use social media as part of your job duties for Euronet's marketing, public relations, recruitment, corporate communications, investor relations or other business purposes, you should carefully review the following.

Note that Euronet owns all social media accounts used on behalf of Euronet or otherwise for business purposes, including any and all login information, passwords and content associated with each account, such as followers and contacts. Euronet owns all such information and content regardless of the employee that opens the account or uses it and will retain all such information and content regardless of separation of any employee from employment with Euronet. Before creating a social media account that will be used on behalf of the Company, please contact the investor relations department for approval.

If your job duties require you to speak on behalf of the Company in a social media environment, you must still seek approval for such communication from the investor relations department and/or the legal department, who may impose certain requirements and restrictions with regard to your activities. Likewise, if you are contacted for comment about Euronet for publication, including in any social media outlet, direct the inquiry to Euronet's investor relations department and do not respond without written approval.

Social media sites and accounts attract hackers, which can pose a threat to our corporate networks as well as personal computers and mobile devices. A compromised account may also create disclosure risks for the Company. To minimize these risks, you should use a complex password for all social media accounts and periodically review the account to ensure that there is no unauthorized access. Any suspicious or activity should be immediately reported to the IT department.

Guidelines for Employees' Responsible Use of Social Media

The above material covers specific rules, policies, and contractual obligations that employees must follow in using social media, whether for personal or business purposes, in consideration of their employment and subject to discipline for violations. The following sections of the policy provide employees with common-sense guidelines and recommendations for using social media responsibly and safely, in the best interests of Euronet. These guidelines reflect the "duty of loyalty" every employee owes its employer, and are intended to add to, not contradict, limit, or replace, applicable mandatory rules, policies, legal requirements, legal prohibitions and contractual obligations.

Protect the Company's Goodwill, Brands, and Business Reputation You are personally responsible for what you communicate on social media. Remember that what you publish might be available to be read by the public (including the Company itself, future employers, and social acquaintances) for a long time. Keep this in mind before you post content.

Unless a communication to be made on behalf of the Company is approved by the investor relations department, make it clear in your social media activity that you are speaking on your own behalf. Write in the first person and use your personal e-mail address when communicating via social media. Never post anonymously to social media sites when your post could be attributed to Euronet or its stakeholders. Anonymous posts can be traced back to the original sender's email address. Follow all guidelines in this policy regarding social media postings.

If you disclose your affiliation as an employee of Euronet, it is recommended that you also include a disclaimer that your views do not represent those of your employer. For example, consider such language as "the views in this posting do not represent the views of my employer."

Use good judgment about what you post and remember that anything you say can reflect on Euronet, even if you do include a disclaimer. Always strive to be accurate in your communications about Euronet and remember that your statements have the potential to result in liability for yourself or the Company. We encourage professionalism, accuracy and honesty in social media and other communications.

Respect Intellectual Property and Confidential Information.

Euronet's Code of Conduct, confidentiality agreements and employee handbooks restrict employees' use and disclosure of the Company's confidential information and intellectual property (see above). Beyond these mandatory restrictions, you should treat the Company's trade secrets and other confidential information and intellectual property accordingly and not do anything to jeopardize them through your use of social media. In addition, you should avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for yourself and for Euronet.

To protect yourself and the Company against liability for copyright or trademark infringement, where appropriate, reference sources of particular information you post or upload and cite them accurately. If you have any questions about whether a particular post or upload might violate the copyright or trademark of any person or company, ask Euronet's legal department before making the communication.

You should not share confidential or sensitive information without the prior approval of the investor relations department, including disclosure of any dealings with customers, business transactions or contracts. If you are uncertain as to what may be deemed confidential, you should inquire with the legal department or the investor relations department before taking any action.

Respect and Comply with Terms of Use of All Sites You Visit

Do not expose yourself or Euronet to legal risk by using a social media site in violation of its terms of use. Review the terms of use of all social media sites you visit and ensure your use complies with them. If you are using social media as part of your job duties, pay particular attention to terms relating to:

- Prohibitions or restrictions on the use of the social media site, including prohibitions or restrictions on use for advertising, marketing and promotions or other commercial purposes.
- Ownership of intellectual property used on, or information collected or generated through use of, the site (for example, any of the Company's copyrighted material and trademarks that might be posted on the site, or user information the Company collects through the site).
- Requirements for licenses or other permissions allowing use by the site owner and other third parties of the Company's trademarks or other intellectual property.
- Privacy rights and responsibilities of the site owner and users.

Respect Others

Do not post anything that Euronet’s customers, or business partners would find offensive, including ethnic slurs, sexist comments, discriminatory comments, insults, or obscenities.

Supervisors and direct reports should refrain from trying to connect with one another on social media sites. Neither supervisors nor direct reports should feel pressured to accept any requests from anyone at Euronet.

Conduct not Prohibited by this Policy

This policy is not intended to restrict international communications or actions protected or required by applicable local, state or federal law.

Travel & Expense Policy

Expense claims must be submitted promptly—either immediately or after the trip concludes—and no later than 30 days following the end of travel or transaction.

Statement of Policy

This policy provides clear guidelines for incurring and reimbursing travel and business-related expenses.

Employees are expected to exercise the same care and judgment when spending Company funds as they would with their own, ensuring that all expenditures are reasonable, necessary, and aligned with business objectives. The goal is to support safe, cost-conscious, and compliant travel while maintaining transparency and accountability.

Employees may be required to travel or incur expenses as part of their job, which will be reimbursed by the Company. This document outlines the procedures and standards all employees must follow when booking travel and incurring expenses on behalf of the Company.

Our travel policy ensures that travel and expenses are managed fairly, cost-effectively, sustainably, and in compliance with legal and industry standards.

Purpose

The purpose of this policy is to:

- Provide clear instructions for arranging travel and accommodation.
- Outline the approval process for business-related travel expenses.
- Define acceptable expenses and the reimbursement process.
- Promote responsible spending in line with the Company's values, economic interests, and commitment to minimizing environmental impact.
- Ensure compliance with tax regulations and auditing standards.

Scope

This policy applies to all employees who travel or incur expenses for business purposes. Each entity adopting this policy is responsible for adapting details to local laws, conditions, tax regulations, and preferred suppliers. Local policies may be more restrictive, but never less restrictive, than this general policy. Any local policy must be reviewed and approved by the policy owner.

Effective Date

This policy takes effect upon its approval.

Definitions

This section provides clarity and ensures a uniform understanding of key terms used in this policy and process.

- Compliance: Adherence to internal policies, legal regulations, and ethical standards at all stages of the spending and approval process.
- Record-keeping: The systematic documentation and retention of relevant documents for audit, reference, and compliance purposes.
- Company: Refers to Euronet Worldwide Inc. and its subsidiaries.
- Navan: The Company's official travel and expense management platform, providing both a web-based portal and a mobile application to support employees in booking business travel, managing itineraries, and submitting expense reports in a streamlined and compliant manner.

Roles and Responsibilities

This section outlines the key roles and responsibilities of individuals and departments involved in the travel and expense process, ensuring a clear understanding of expectations and accountability.

- Employees: Responsible for adhering to this policy, submitting accurate expense claims, obtaining the necessary approvals, and justifying expenses incurred on behalf of the Company or for reimbursement.

- Managers: Responsible for approving travel bookings and expense claims, verifying the legitimacy and accuracy of charges, and ensuring employees comply with this policy.

General Guidelines

Business travel should be limited and replaced with videoconferencing whenever possible. Employees are encouraged to make cost-conscious and responsible travel choices; Navan rewards such behavior with points that can be redeemed for personal travel.

Employees should always use the most economical rates available when booking travel. Ground transportation should be used judiciously, with a preference for public transportation or shared services over taxis or car rentals. No more than five employees from the same department or management level within a single business unit may travel together on the same aircraft or vehicle.

Expenses should be claimed in the currency in which they were paid. Reimbursement will be made in the employee's home-market currency. Employees may use the exchange rate applied to their company or personal credit card and may claim any associated currency exchange fees.

Failure to comply with this policy may result in denial of reimbursement and/or appropriate management action, up to and including termination of employment.

Travel Booking Procedure

This section provides guidelines for arranging business travel and ensures that all travel is authorized in accordance with the Company's Delegation of Authority Policy.

Travel plans should be made as far in advance as possible to take advantage of better rates. Accommodation booked outside the recommended timeframe require manager approval. Last-minute bookings, which often incur higher costs, should be avoided unless strictly necessary. Any subsequent modifications to the travel schedule must be made officially by the original requester or a delegated travel office assistant. Manager approval is required for any changes that increase the cost beyond the originally approved amount.

All company travel must be booked through Navan, the Company's official travel and expense platform. All business travel must receive prior approval from the employee's manager before being booked. Any travel reservations made without such approval may be subject to cancellation or will not be eligible for reimbursement. Approval must be documented before finalizing travel arrangements.

The Company does not cover weekend hotel stays or meals unless it is more cost-effective than a round-trip flight or there is a valid business reason, such as conducting business over the weekend. For booking assistance or support while traveling, employees should use the following contact options:

- Navan App or Website: Employees are encouraged to manage bookings and changes directly through the Navan mobile application or online portal.
- 24/7 Support: Navan provides round-the-clock customer service for urgent travel issues, itinerary changes, or disruptions. Contact information is available within the Navan platform.
- Emergency Assistance: In case of a travel-related emergency, employees should use the emergency contact option within the Navan app or call the dedicated emergency hotline listed in their travel confirmation.

Employees are responsible for ensuring their travel profiles (e.g., passport details, frequent flyer numbers, and payment methods) are kept current within Navan.

Step-by-Step Booking and Claim Process

Employees must first arrange all airfare, hotel, car, or other transportation bookings through the Navan platform. During the business trip, employees are encouraged to upload invoices and receipts to the

Navan app or web portal. All original invoices and receipts must be collected and retained.

Travel expense claims will be submitted to the employee's manager for approval. Once approved, the Finance Department will validate the claims and, if no issues are identified, submit the report for payment. Reimbursement will be made directly to the employee's bank account following Finance Department approval.

Airfares

Employees should book flight tickets at least 14 days in advance. Bookings made later require manager approval.

Non-refundable fares should be used whenever possible to reduce costs; refundable fares are allowed only when business requirements or risk considerations make them necessary.

Cabin upgrades are permitted if cost-effective and within the maximum allowed cabin class. Seat upgrades within the same cabin are allowed, with manager approval if needed.

Employees using their own vehicles for business travel must drive safely and comply with all applicable local traffic laws. Mileage expenses will be reimbursed at the applicable rate per mile or kilometer, inclusive of all vehicle-related costs, such as insurance, fuel, tires, and routine maintenance.

Employees should book economy for short-haul flights (≤11 hours) and premium economy for long-haul flights (>11 hours). Manager approval is required if upgrades are needed due to availability.

Employees are responsible for reviewing ticket terms and conditions, including refund policies and baggage allowances, to ensure travel meets business needs in the most cost- effective manner

Railways

Employees should book train travel in advance. Any changes to the itinerary must be made through the same booking method and require manager approval.

Non-refundable fares should be used whenever possible, as they are typically less expensive than refundable fares. Refundable fares may be booked only when business requirements or risk considerations make them necessary. Employees should book Standard Class tickets unless otherwise approved by a manager.

Hotels

Hotel accommodation will be reimbursed only when an overnight stay is necessary for business purposes. Employees should book hotels at least 14 days in advance.

Standard accommodation should be booked in refundable rooms whenever possible. Non-refundable bookings may be permitted only when cost-effective or required by business circumstances.

Costs for weekend stays are generally not covered, unless:

- Business activities occur during the weekend,
- The trip lasts more than one week, or
- Staying over the weekend is less expensive than a round-trip flight.

If a business trip is canceled, employees must cancel hotel reservations promptly and within the hotel's cancellation policy deadlines to minimize penalties.

Vehicle Rental

Employees may book rental vehicles when traveling for company business, provided the vehicle is within the allowed price range set in Navan. Rentals should be booked at least 14 days in advance. Employees traveling together are expected to share a vehicle whenever practical. Luxury or premium vehicles are not permitted under this policy, although bookings for a premium chauffeur-driven vehicle (black car) are allowed when necessary. Company insurance covers rental vehicles, so additional or extra insurance should not be purchased. If an accident occurs and the employee is determined to be at fault, they may be liable for the deductible portion.

Ground Transportation (bus, taxi, shuttle, public transport)

Employees are encouraged to use public transportation, such as buses, trams, and subways, whenever feasible, safe, and practical. Taxis or ride-sharing services (e.g., Uber) may be used when public transportation is not convenient, available, or cost-effective. Only registered taxis or reputable ride-sharing services should be used.

For airport transfers and travel to and from business meetings, employees may arrange their own transportation, ensuring safety and cost-effectiveness. When traveling abroad, employees should contact the local travel office for guidance on approved taxi or shuttle services.

Personal Car & Mileage Reimbursement

Employees should avoid using personal vehicles for business trips whenever possible. Employees with access to a company car or a car allowance are expected to use those instead and are not eligible to claim fuel or mileage for personal vehicles.

If the use of a personal vehicle is necessary, employees must obtain prior approval from their manager. Approval should be based on the necessity and cost-effectiveness of using a personal vehicle compared to other transportation options. Reimbursement will be provided in accordance with local tax laws.

Reimbursement applies only to mileage incurred strictly for business purposes. The reimbursement rate per mile or kilometer is determined by the employee's home country tax authority(as published in Rydoo or another official source). Where available, the applicable rate is preloaded in Navan. If no home country rate is available a general rate will be used. Expense claims must include: the date of travel, trip start and end locations, businesses or sites visited, and total miles or kilometers traveled.

Other Car-related Expenses during Business Travel (parking, tolls, fuel)

Employees may be reimbursed for necessary car-related expenses incurred during business travel. This includes parking fees at airports, hotels, or business locations, provided that such parking is required and represents the most cost- effective option. Tolls paid during business travel are also reimbursable. Reimbursement should be limited to expenses directly related to business purposes and must be supported by valid receipts.

Meals & Entertainment

Personal Meals

Employees may claim reimbursement for actual meal expenses incurred during business travel, up to the daily per diem limits set by the employee's home country tax authority for the travel destination (as published in Rydoo or another official source). Employees are expected to spend reasonably and not treat the per diem as a target amount. You may reclaim a daily food allowance up to USD 80 supported by receipts or the equivalent in local currency if travelling overseas. If breakfast is included in the hotel rate, it must be deducted from the daily allowance.

Business Meals / Entertainment

Meals involving external business partners are considered Entertainment. External partners must have a potential or actual business relationship with Euronet that benefits the company. All entertainment costs must be reasonable and comply with:

- Euronet's anti-bribery and corruption policies, as well as those of the partner company
- Applicable local laws and regulations

Note: Government officials may never be entertained, as this could constitute a public offence.

Alcohol

Wine and beer may be included if customary and permitted by local practices. Spirits or cocktails are not permitted unless they form part of the meal or event.

Tips & Service Charges

Tips and service charges may be included if they are customary in the country of travel and remain reasonable.

Payment & Approvals

The most senior employee present at a meal or event is responsible for settling the bill. Entertainment limited to internal employees is considered a Team Building activity and requires prior approval from a Manager.

Travel Insurance

Euronet provides coverage for illnesses and injuries resulting from accidents during business travel. Employees should refer to the Global Travel Insurance Policy for full details. In the event of a medical issue while traveling, employees should contact our insurance partner GeoBlue to initiate a claim. Euronet will be notified to verify the claim.

Employees are advised to carry the GeoBlue contact information while traveling:

- Policyholder: Euronet Worldwide, Inc.
- Policy Number: 9117046
- Toll-Free (within the U.S.): 1-877-244-6871
- Collect/Reverse Charge (outside the U.S.):
- +1-715-346-0859
- Email: assistance@aig.com

Most accidental injuries and illnesses are covered by this insurance. If an employee must pay any medical expenses upfront, reimbursement can be claimed by submitting the relevant invoices along with any supporting medical documentation.

Other Reimbursable Business Expenses

The following categories represent the most common other business expenses eligible for reimbursement when incurred. All expenses must be reasonable, necessary, and supported by appropriate documentation (e.g., itemized receipts, invoices, or booking confirmations).

Business Communications: Telephone calls, internet access fees, mobile roaming charges, and other communication costs directly related to conducting business.

Conference or Event Fees: Registration costs for approved business conferences, seminars, or training events. Conferences, donations, gifts (internal and external), and miscellaneous discretionary expenses are reimbursed per transaction and must align with business purpose guidelines.

Professional Memberships and Subscriptions: Professional memberships and subscriptions expenses that support you in fulfilling your role and duties. If you are in any doubt about whether or not a professional membership or subscription is reclaimable through expenses, you should speak to your manager first.

Other Necessary Expenses: Reasonable costs directly related to business purposes, subject to prior managerial approval. Covered benefits include internet access, office supplies, shipping/postage, marketing, software, licenses/registrations and tools/materials.

All benefit-related reimbursements are made per transaction unless noted otherwise.

Expenses not expressly listed above may be considered on a case- by-case basis but require justification and pre-approval. Hardware, subscriptions, and tolls are reimbursed per transaction.

Non-Reimbursable Expenses

The following categories of expenses are considered personal in nature or outside the scope of necessary business travel and will not be reimbursed under any circumstances:

Personal Entertainment: Movies, in-room entertainment, sporting events, concerts, sightseeing tours, or other leisure activities.

Luxury or Upgrades: First-class or business-class airfare, luxury hotel accommodations, vehicle upgrades, or other premium services not pre-approved.

Personal Items: Toiletries, clothing, luggage, or other personal articles.

Fines and Penalties: Traffic tickets, parking fines, or other penalties incurred while traveling.

Companion Travel: Costs associated with spouses, family members, or other non-business companions. Childcare or Pet Care: Expenses for dependents or pets while on travel.

Lost or Stolen Items: Replacement of personal items or cash lost or stolen during travel.

Unapproved Expenses: Any costs incurred without prior managerial authorization, where required.

Employees are expected to exercise good judgment and cost- consciousness when incurring travel expenses. Failure to comply with this policy may result in denial of reimbursement.

Reimbursement

All expenses must be submitted with sufficient detail to explain the business purpose and approved in accordance with this policy. Once approved and validated by the Finance Department, reimbursement will be issued to the employee's bank account, typically within five business days.

Cash Advances

In special circumstances, such as last-minute travel, emergencies, or significant changes in travel plans (for example, when an employee does not have sufficient time to arrange a corporate credit card or personal funds), employees may request a cash advance to cover necessary expenses. Pre- approval from the Regional Finance Director is required and must be obtained via email.

The approval request should include a reasonable estimate of the expected business expenses for the trip, along with a brief explanation of the business purpose and how the expenses relate to company activities.

Corporate Credit Cards

Corporate credit cards are issued to employees who frequently travel or incur significant business expenses, with eligibility determined by the employee's role and responsibilities. Employees holding a corporate card must ensure that all expenditures are supported by an invoice or receipt and included in an expense claim submitted through Navan. Any expenditure lacking proper documentation or not approved by the employee's manager may be considered a personal expense and could be deducted from the employee's payroll.

Corporate credit cards must be used exclusively for business- related expenses, including travel, accommodation, meals, and other approved expenditures. Personal expenses, cash advances, and non-business-related purchases are strictly prohibited. The Finance department will periodically audit corporate card usage to ensure compliance with this policy. Any discrepancies will be investigated and addressed appropriately.

If a corporate credit card is lost or stolen, the cardholder must immediately notify both the issuing bank and the Company's Finance department. Cardholders are not liable for any unauthorized charges incurred after the card has been reported lost or stolen, provided the incident is reported promptly.

Document Requirements

All employees must provide original invoices or receipts for all expenses claimed. Expense claims should be submitted and documented in Navan.

Invoices or receipts should be issued to the employee's legal entity and include the following information:

- Invoice date
- Vendor's legal and contact information
- Euronet's legal entity information

- Detailed description of the goods or services provided
- Total amount due and payment terms
- Confirmation of payment received (e.g., a stamp or note indicating payment)

If an invoice or receipt is lost, employees must provide a written explanation along with any available alternative proof of payment, such as a credit card or bank statement. Receipts are acceptable only when an invoice cannot be obtained, for example, for ground transportation tickets.

Policy Violation Escalation Procedure

In the event of a policy violation, the Finance Department will investigate and propose appropriate actions (e.g., partial or full denial of reimbursement, formal notice) to the Managing Director and HR Department for review.

Repeated or serious violations may result in escalating consequences, depending on severity and frequency, including:

- Formal Warning: Written notification outlining the violation(s) and the requirement for compliance.
- Reimbursement Denial or Access Restriction: Non-eligible expenses will not be reimbursed, and access to Navan may be restricted.
- Disciplinary Action: Persistent non-compliance may result in disciplinary measures, including suspension.
- Termination: Severe or fraudulent violations may result in termination of employment.
- Legal or Regulatory Action: If a violation involves fraud, dishonesty, or misconduct of a criminal nature, the Company reserves the right to refer the matter to external legal or regulatory authorities.

Employees are expected to comply with this policy to ensure expense claims are processed smoothly and in accordance with Company standards. If there is uncertainty about eligibility, employees should seek clarification from their Manager before incurring the expense

Auditing and Compliance

The Finance department has the right to conduct periodic ad- hoc internal audits of the expenses incurred. These audits will be conducted randomly to prevent predictability. Following an audit, a report will be prepared identifying any discrepancies or instances of non-compliance.

Immediate corrective actions will be taken as appropriate, which may include:

- Requiring reimbursement for unauthorized expenses
- Providing additional training on the travel and expense policy
- Implementing disciplinary measures

Documentation and Recordkeeping

Euronet will maintain proper documentation of reconciliations, discrepancies, and supporting records. In line with recordkeeping standards, Euronet will ensure that all records are accurate, complete, consistent, and organized, making them readily accessible for review and audits.

<u>Retention Period:</u> Records and documents will be retained for at least seven years, or longer if required by applicable law, even after a transaction is completed or a contract is terminated.

<u>Controlled Access:</u> Access to records will be restricted to authorized personnel under the need-to-know principle. Any requests for access by others must be made in writing and approved by the Policy Owner.

<u>Data Protection:</u> All documentation will be managed in compliance with applicable data protection and financial recordkeeping regulations, including the EU General Data Protection Regulation (GDPR), the U.S. Sarbanes-Oxley Act (SOX), and any other relevant local privacy or financial reporting laws.

In addition, the Company will comply with any other applicable data protection, financial reporting, and recordkeeping requirements in the jurisdictions in which it operates. Where local laws impose stricter standards, those standards shall apply.

Whistleblower Policy

Purpose

The purpose of this Whistleblower Protection Policy is to encourage and protect employees of Euronet Worldwide, Inc. (the "Company") who report suspected misconduct, illegal activities, or violations of the Company's policies.

This policy aims to create a culture of transparency, accountability, and integrity within the Company, and to ensure that employees feel safe and supported when reporting concerns.

The Company is committed to the highest standards of ethical and legal conduct and believes that encouraging and protecting whistleblowers is essential to maintaining these standards.

Scope

This policy applies to every Euronet employee, contractors, suppliers or any other member of staff. We expect all employees, and other members of staff, to familiarize themselves with this policy, and to act in accordance with it in the performance of their duties and responsibilities. Failure to comply with this policy may subject Euronet, its employees and staff to civil and/or criminal liability. Employees or any other members of staff who fail to comply with this policy will be subject to disciplinary action up to and including termination of employment. It covers all reports of suspected misconduct, illegal activities, or violations of the Company's policies, whether made internally or externally.

The policy also applies to any third parties who may be involved in the reporting or investigation process, such as legal counsel, auditors, or regulatory authorities.

Protected Disclosures

Employees are encouraged to report any suspected misconduct, illegal activities, or violations of the Company's policies, including but not limited to:

- Financial irregularities or fraud, such as false accounting, embezzlement, or misappropriation of funds
- Corruption or bribery, including kickbacks, favors, or gifts intended to influence business decisions.
- Harassment or discrimination based on race, gender, age, religion, political preference or any other protected characteristic. Health and safety violations that pose a risk to employees, customers, or the public.
- Environmental damage or non-compliance with environmental regulations Insider trading or other securities law violations
- Any other illegal or unethical conduct that may harm the Company, its employees, or its stakeholders.

Reporting Procedure

Employees should report their concerns to the HR Department, which may include a supervisor, human resources representative, legal counsel, or a dedicated whistleblower hotline.

Reports can be made in person, by phone, or in writing, and should include as much detail as possible about the suspected misconduct or violation.

Anonymous reports will also be accepted and investigated to the extent possible, but employees are encouraged to identify themselves to facilitate follow-up and investigation.

The Company will acknowledge receipt of all reports and keep the whistleblower informed of the progress and outcome of the investigation, to the extent possible.

Investigation

All reports will be promptly and thoroughly investigated internally, which may include internal or external legal counsel, auditors, or other experts, as necessary.

The investigation will be conducted in a fair, objective, and unbiased manner, and will seek to gather all relevant facts and evidence.

The identity of the whistleblower will be kept confidential to the extent possible and will only be disclosed on a need-to- know basis to those involved in the investigation.

The Company will take appropriate corrective action based on the findings of the investigation, which may include disciplinary action, termination of employment, or referral to law enforcement or regulatory authorities.

Protection from Retaliation

The Company prohibits any form of retaliation against employees who make a good faith report of suspected misconduct or participate in an investigation.

Retaliation may include, but is not limited to, termination, demotion, suspension, threats, harassment, or any other adverse employment action.

Any employee who engages in retaliation will be subject to disciplinary action, up to and including termination of employment.

Employees who believe they have been subjected to retaliation should report it immediately to the HR Department, and the Company will promptly investigate and address any such reports.

The Company will also provide appropriate support and protection to whistleblowers, such as legal representation or counseling services, as needed.

Confidentiality

The Company will maintain the confidentiality of the whistleblower's identity to the extent possible and will only disclose it on a need-to-know basis to those involved in the investigation or as required by law.

All employees involved in the reporting or investigation process are expected to maintain strict confidentiality and not discuss the matter with anyone outside of the designated channels.

Any breach of confidentiality will be subject to disciplinary action, up to and including termination of employment.

The Company will also protect the confidentiality of any documents or evidence related to the investigation and will store them securely with restricted access.

False Reports

Employees who knowingly make false reports or provide false information during an investigation may be subject to disciplinary action, up to and including termination of employment.

False reports include those made in bad faith, with malicious intent, or with reckless disregard for the truth. Employees are expected to report concerns honestly and accurately, and to cooperate fully with any investigation. However, employees who make reports in good faith will not be subject to disciplinary action, even if the concerns are not substantiated by the investigation.

Training & Awareness

The Company will provide regular training to all employees on this Whistleblower Protection Policy and their rights and responsibilities under it.

The training will cover the purpose and scope of the policy, the reporting procedure, the investigation process, and the protections against retaliation.

The training will also emphasize the importance of ethical conduct and the Company's commitment to transparency and accountability.

The policy will be prominently displayed in the workplace, on the Company's website, and in other relevant communications, and will be included in the employee handbook and orientation materials.

The Company will also provide additional resources and support to employees who have questions or concerns about the policy or the reporting process.

Review & Amendment

This policy will be reviewed annually by HR to ensure its effectiveness and compliance with applicable laws and regulations.

The review will consider any changes in the Company's operations, legal requirements, or best practices, and will seek feedback from employees, stakeholders, and external experts as appropriate.

Any amendments to the policy will be communicated to all employees and will be subject to approval by the Company's board of directors or other governing body.

The Company reserves the right to modify or terminate this policy at any time but will provide reasonable notice and transition procedures to employees in the event of any significant changes.

Reference

Appendix A
Anti-Bribery Program Compliance Manual

1. INTRODUCTION

The purpose of this Manual is to provide all employees, officers, directors and representatives of Euronet Worldwide, Inc. and its subsidiaries ("EWI" or the "Company") with the tools and resources necessary to enable,monitor and enforce the Company's full compliance with the United States Foreign Corrupt Practices Act ("FCPA"),the U.K. Bribery Act, and applicable anti-bribery laws in the countries in which the Company conducts business("Anti-Bribery Laws").

2. CORPORATE POLICIES

2.1 Anti-Bribery Policy Statement

EWI has adopted a policy on compliance with Anti-Bribery Laws (the "Policy"). The Policy, which is attached as Annex A to this Manual, applies to the Company and all employees, officers, directors and representatives of the Company.

2.2 Code of Business Conduct and Ethics

The Policy and this Manual supplement the EWI Code of Business Conduct & Ethics ("Code of Conduct") adopted by the Board of Directors on September 14, 2011, as amended through the date of this Manual. All provisions of the Code of Conduct remain fully effective.

2.3 Anti-Bribery Compliance Program and Manual

The Anti-Bribery Compliance Program described in this Manual ("Compliance Program") is intended to facilitate implementation of the Policy and provide detailed guidance and procedures which will allow all Company employees, officers, directors and representatives to efficiently and effectively carry out the Policy's requirements and objectives. The Manual will be periodically reviewed by the General Counsel and/or the Board and appropriate amendments will be issued as often as necessary.

3. ADMINISTRATION OF COMPLIANCE PROGRAM

3.1 Board of Directors

The Board of Directors of EWI (the "Board") has ultimate responsibility for ensuring that the Company meets its obligations under Anti-Bribery Laws. The Board will evaluate and adopt possible amendments to the Policy and the Manual and other aspects of the Compliance Program. The Board has delegated certain responsibilities to its Audit Committee ("Audit Committee") and to certain officers of the Company as specified in the Manual and the Audit Committee Charter.

3.2 Audit Committee

The Audit Committee has responsibility for:

(a) overseeing administration of the Compliance Program;
(b) reviewing the findings of the General Counsel and/or the Compliance Officer regarding possible violations of the Policy or the Compliance Program and reviewing the findings of internal audits regarding possible bribery; and
(c) where the circumstances warrant, undertaking an independent investigation of possible violations of the Policy or the Compliance Program.

3.3 General Counsel

The General Counsel has responsibility for:
(a) assisting the Compliance Officer, as needed, in respect of the Policy and the Compliance Program;
(b) advising Company personnel (as EWI's legal counsel) on any legal issues related to compliance with the Policy;
(c) referring to Compliance Officer questions, reports and/or complaints the General Counsel receives regarding adherence to the Policy and the Compliance Program;
(d) immediately reporting to the Compliance Officer and the Audit Committee any material violations of the Policy or the Compliance Program that appear to have occurred; and

(e) assisting the Compliance Officer in investigating possible violations of the Policy and the Compliance Program unless the Audit Committee determines that an independent investigation is warranted.

In carrying out the foregoing responsibilities, the General Counsel may utilize the assistance of qualified staff members, investigators, forensic accountants and outside legal counsel.

3.4 Compliance Officer

The Compliance Officer has responsibility for:

(a) day-to-day administration of the Policy and the Compliance Program;
(b) coordination of anti-bribery education and training programs as required by the Compliance Program;
(c) providing any pre-approval required for payments or incurrence of expenses when such pre-approval is required under the Compliance Program;
(d) receiving and responding to questions, reports and/or complaints regarding adherence to the Policy and the Compliance Program, after consultation with the General Counsel and/or the Audit Committee where required by this Manual or otherwise appropriate;
(e) annual review of published international anti-bribery risk indices (such as Transparency International's CPI) and based on them, making recommendations and administering any additional compliance measures considered appropriate in high risk countries;
(f) providing information and recommendations to the Company's internal audit department regarding auditing of Anti-Bribery Policy compliance;
(g) administration of the hotline maintained for reporting anti-bribery violations;
(i) immediately reporting to the General Counsel the Audit Committee any material violations of the Policy or the Compliance Program that appear to have occurred; and
(j) reporting to the General Counsel at least annually on the status of the Company's compliance with the Policy and the Compliance Program and any practical issues that have arisen in connection with administration of the Policy or the Compliance Program.

The Compliance Officer is authorized to communicate directly with the Audit Committee at any time.

3.5 Internal Auditors

The Internal Audit Department will assist with enforcement of the Policy and the Compliance Program by routinely and regularly including in the internal audit process questions and reviews designed to test and verify compliance with the Policy and the Compliance Program and by otherwise assisting the Compliance Officer with administration of the Compliance Program as required from time to time. Each Internal Auditor will immediately notify the Compliance Officer, the General Counsel or the Audit Committee, as appropriate, when any credible indication of a failure to comply with the Policy or the Compliance Program comes to his or her attention.

3.6 Hot Line Programs

The Company will maintain telephone and electronic mail and postal mail hotlines dedicated to direct communication with the Compliance Officer regarding compliance with the Policy and the Compliance Program. These hotlines may be the same as that maintained under the Company's Code of Conduct. All Company personnel will be made aware of the existence and availability of the hotlines. All Company personnel are encouraged to report any potential violation of the Policy or the Compliance Program via one of the hotlines. Reports may be made anonymously if so desired. The Company's Non-Retaliation Policy covers anyone submitting information about a potential violation of the Policy, the Compliance Program, laws, regulations, or the Code of Conduct. There will be no reprisal for the submission of any information or report that is submitted in good faith.

The Compliance Officer will be appointed from time to time and identified to all personnel.

The current Compliance Program hotline is:
Telephone: + 1-972-708-5030
Email: hotline@eeft.com
Postal: Compliance Officer
Euronet Worldwide, Inc.
3500 College Boulevard
Leawood, Kansas 66211 USA

3.7 Management's Responsibility

A list of key managers with responsibility for the management of principal business units or functions will be maintained by the Compliance Officer, the General Counsel and/or the CFO, and such management will:

(a) ensure that their business units or functions disclose to the Compliance Officer any business partners (including customers, suppliers and other contracting parties) in which a government has a 30% or greater shareholding or may otherwise be considered a "government enterprise" as described in Section 9.1 so that appropriate measures can be taken with respect to those partners to ensure compliance with the Policy.
(b) ensure that any pre-approval required under Section 9.1 of this Manual is obtained prior to the incurrence of the expense, payment or gift that is subject to pre-approval.

Any violation of the Policy or this Manual by any employee may be grounds for discipline, up to and including dismissal of the employee.

4. EDUCATION AND TRAINING

The Compliance Officer will either conduct or arrange anti-bribery training sessions for Company personnel as frequently as he deems appropriate to ensure proper awareness of and compliance with Anti-Bribery Laws and this Manual. Completion of such training shall be required at least once every two years for key Company management and accounting personnel, as well as any other personnel identified by the Compliance Officer as having responsibilities that require particular focus on Anti-Bribery Laws. The form and scope of such training shall be determined by the Compliance Officer.

5. DUE DILIGENCE PROCEDURES

5.1 Acquisitions

Whenever the Company pursues the acquisition of any business entity, the due diligence process associated with the proposed acquisition shall include an investigation of the acquisition target's compliance with the Anti-Bribery Laws. The specific information to be obtained in connection with such investigation shall be determined by, and the results of such investigation shall be reviewed and approved by, the Compliance Officer and the General Counsel.

5.2 Joint Ventures

Whenever the Company enters into any joint venture outside the United States, a review shall be conducted of the prospective joint venture partner or partners in order to determine the reputation, beneficial ownership,professional capability and experience, financial standing and credibility of the prospective joint venture partner or partners and, to the extent reasonably available, the history of such prospective joint venture partner's or partners' compliance with applicable provisions of Anti-Bribery Laws. The specific information to be obtained in connection with such investigation shall be specified by, and the written results of such investigation shall be reviewed and approved by, the Compliance Officer and the General Counsel.

5.3 Consultants, Agents, Sponsors and Other Representatives

Before any agreement is signed with a consultant, agent (excluding Ria or epay agents that are part of their product distribution networks, whose selection in the ordinary course shall be subject to their standard compliance procedures), sponsor or other independent third party representative in connection with any business being sought or transacted outside the United States, an investigation shall be conducted of the prospective representative in order to determine the reputation, beneficial ownership, professional capability and experience, financial standing and credibility of the prospective representative and, to the extent reasonably available, the history of such prospective representative's compliance with applicable provisions of Anti Bribery Laws. The specific information to be obtained in connection with such investigation shall be determined by, and the results of such investigation shall be reviewed and approved by, the Compliance Officer or the General Counsel. When the Compliance Officer or the General Counsel deems it appropriate or necessary, the investigation shall include a personal interview of the prospective representative by a designee of the Compliance Officer or a designee of the General Counsel.

5.4 Red Flags

One of the key aspects of due diligence investigations related to compliance with Anti-Bribery Laws is the identification of "red flags" which may indicate the existence of a potential bribery problem. The FCPA "red flags" identified by the U.S. Justice Department are described in Annex B hereto. Any due diligence investigations conducted by the Company will include an analysis of potential "red flag" issues.

6. CONTRACT PROCEDURES

6.1 Standard Forms and Provisions

The Legal Department has developed forms for many types of contracts and transactions. Where any such form exists, all Company personnel will use such forms unless otherwise agreed by a member of the Legal Department. As part of the Legal Department's review of contracts in accordance with the Company's Policy on Legal Review of Contracts, the Legal Department will determine whether the business relationship covered by a contract includes appropriate provisions to ensure compliance with Anti-Bribery Laws.

The Company shall attempt to include in any consultancy or agent agreement of the type referred to in Section 5.3 provisions substantially similar to those specified in Annex C in respect of the following matters:

(a) Application of and Compliance with Anti-Bribery Laws
(b) Restriction on Government and Political Activities
(c) Accuracy of Documents
(d) Cooperation with Audit Activities
(e) Remedies for Default
(f) Payment Mechanisms

In addition, all contracts which provide for the disbursement of funds by the Company to another contract party for business development services related to business transactions outside the United States shall be in writing and shall require the other party to submit a written invoice. Contracts requiring the disbursement of funds by the Company for such services shall also require that funds shall be transferred only to a bank account owned by the designated recipient and that such account shall be located in the jurisdiction where the relevant business services are to be performed unless the General Counsel determines that payment in another jurisdiction does not violate local law and that a valid business reason for payment in another jurisdiction exists.

6.2 Approval Requirements

In addition to any other approvals required by other Company policies, any contract to which the second or third paragraphs of Section 6.1 above applies shall require the specific approval of the General Counsel or the Compliance Officer.

7. THIRD PARTY ISSUES

Anti-Bribery Laws prohibit corrupt payments through intermediaries. Persons and entities covered by Anti-Bribery Laws are liable for indirect payments or promises prohibited by Anti Bribery Laws if such payments or promises are made through a consultant, agent, sponsor, job, venture partner or other third party with the knowledge that the ultimate beneficiary is a prohibited recipient. Knowledge includes conscious disregard and deliberate ignorance of facts which indicate a high probability that the relevant payment will occur.

If any Company personnel knows or reasonably believes that a payment or promise of payment prohibited by Anti-Bribery Laws has been, is being or may be made by a joint venture partner, representative or other third party intermediary for or on the Company's behalf or for the benefit of the Company, the relevant individual shall immediately advise the Compliance Officer or the General Counsel and shall use all reasonable efforts to prevent the payment or promise of payment from occurring.

8. AUDITING

8.1 Regular Auditing

Testing and analysis of Company transactions for possible violation of Anti-Bribery Laws, the Policy or the Compliance Program shall be a regular part of the Company's routine audit process and all Company personnel shall cooperate fully with the Company's audit staff in that regard.

8.2 Anti-Bribery Spot Auditing

The Director of Internal Audit and the Compliance Officer shall select at least two Company operating locations outside the United States each year for a special audit of their disbursement and anti-bribery compliance practices. The Audit Department shall maintain a list of procedures that will be applied in such special audits.

8.3 Anti-Bribery Audit Reporting to Audit Committee

The results of all anti-bribery auditing activities shall be communicated to the Audit Committee promptly after completion of the relevant audit.

9. ACCOUNTING ISSUES

9.1 Certain Expenses Subject to Pre-Approval

The following payments or expenses shall not be made or incurred without the specific preapproval of the Chief Financial Officer, the Compliance Officer, the General Counsel or any other officer designated by one of them:

(a) Any payment to any government official or any employee of a government enterprise or a commercial enterprise;
(b) The incurrence of any expense (especially for travel or entertainment) on behalf of a government official or an employee of any government enterprise;
(c) Except as provided in the next sentence, the incurrence of any expense (especially for travel or entertainment) on behalf of an employee of a commercial enterprise. Customary travel and entertainment expenses incurred for the purpose of promoting Euronet's products or services, administering contracts or other proper business purposes that are reasonable in amount shall not be subject to pre-approval.
(d) Any gift to any government official or any employee of a government or commercial enterprise with a value exceeding $100 or any lesser amount established in a local Euronet Gift Policy.

For purposes of the Policy and this Manual, a "government enterprise" means an enterprise in which a government owns 30% or more of the voting capital or which might otherwise be considered to be controlled by a government,for example, though the power to appoint directors to the governing board of that enterprise. In the event there is any doubt concerning whether an entity is a "government enterprise," you should consult the Compliance Officer or the General Counsel before making any payment or gift or incurring any expense.

9.2 Materiality Issues

The books and record keeping provisions of the FCPA require that books, records and accounts, including documentation of expenses, are made and kept in reasonable detail and that they accurately and fairly reflect the transactions and disposition of assets of the Company. This standard requires a level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs. That standard is generally thought to be more exacting than the materiality standard which typically applies in accounting and disclosure to investors. Accordingly, even relatively small payments or gifts may have to be accurately recorded in order to satisfy the books and records requirements of the FCPA and other Anti-Bribery Laws.

9.3 Reporting

Any perceived failure of the Company's books and records to meet the requirements of applicable Anti-Bribery Laws must be reported to the Compliance Officer, who shall consult with the Chief Financial Officer, the General Counsel,the Company's internal and external auditors and/or the Audit Committee in order to determine whether a possible violation exists and, if so, the appropriate actions required.

RED FLAGS

1. The contracting party has a history of improper payment practices.
2. The transaction or the contracting party is in a country where there is widespread corruption.
3. The transaction or the contracting party is in a country that has a history of bribes and kickbacks.
4. The transaction or the contracting party is involved in or with an industry that has a history of violations of Anti-Bribery Laws.
5. The contracting party refuses to agree in writing to comply with applicable Anti-Bribery Laws.
6. The contracting party has a family or business relationship with a government official.
7. The contracting party has a poor business reputation.
8. The contracting party insists that its identity remain confidential or refuses to divulge the identity of its owners.
9. A government customer recommends or insists on use of a particular intermediary or consultant.
10. The contracting party does not have offices or a staff.
11. The contracting party does not have significant experience.
12. The contracting party insists on unusual or suspicious contracting procedures.
13. The fee or commission to be paid to the contracting party is unusually high, stated in round amounts, single one-time payments.
14. The payment mechanism to be utilized is secretive or unusual.
15. The contracting party submits inflated or inaccurate invoices.
16. The contracting party requests cash or bearer instrument payments.

17. The contracting party requests payment in a jurisdiction outside its home country that has no relationship to the transaction,or the entities involved in the transaction.
18. The contracting party asks that a new customer be granted an excessive credit line.
19. The contracting party requests unusual bonus or special payments.
20. The contracting party requests an unusual advance payment.

STANDARD CLAUSES FOR AGENT AGREEMENTS

(a) **Agent** warrants and represents to the Company that neither **Agent** nor any of its officers, directors, employees,agents or other representatives has or will make any payments of money, or anything of value, nor will such be offered, promised or paid, directly or indirectly, to any foreign officials, political parties, party officials, candidates for public or political party office or representatives of business organizations, to influence the acts of such officials,political parties, party officials, candidates or representatives in their official or representative capacity, to induce them to do any of the following on behalf of the Company:

(i) use their influence with a government to obtain or retain business or gain an improper advantage in connection with any business activities of the Company; or

(ii) improperly perform a function that is public in nature or connected with a business and results in an improper advantage for the Company.

(b) If **Agent** breaches any of the covenants set forth in clause (a), above,

(i) this Agreement shall become void;

(ii) the Company shall have a right of action against **Agent** for the amount of any monetary payment or thing of value made or given by **Agent** in breach of any of such covenants;

(iii) all obligations by the Company to pay any Fee or other compensation to **Agent** shall cease immediately;

(iv) **Agent** agrees to indemnify Company for all liability, costs and fees (including but not limited to attorneys' fees and costs of any investigation) arising from **Agent's** breach of the covenants set forth in clause (a), above, and (iv) the Company may at its sole discretion, rescind this Agreement and **Agent** shall immediately return to the Company any Fee paid to **Agent** arising from any transaction in violation of clause (a) above.

(c) Further, **Agent** agrees to the following:

(i) **Agent** will fully cooperate in any investigation regarding alleged violations of the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act or any applicable anti-bribery or anti-corruption law in connection with performance of this Agreement;

(ii) **Agent** will not employ any subcontractors, sub-agents or consultants in performance of this Agreement without the express,advance written approval of the Company;

(iii) Company may audit all of the **Agent's** books and records of all transactions related to the **Agent's** performance under this Agreement;

(iv) **Agent** acknowledges that the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act apply to this Agreement and all actions taken in performance of this Agreement;

(v) If deemed appropriate by the Company,

(A) **Agent** agrees to have all of its senior level management take the Anti Bribery training provided by the Company;

(B) **Agent** will sign an annual certification stated that the **Agent** has not engaged in any actions on behalf of the Company that has violated the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act or any applicable anti-bribery or anticorruption law; and

(vi) **Agent** has disclosed to Company in writing the names of all persons and entities who have a beneficial ownership in the **Agent**. **Agent** will immediately notify Company in writing in the event any change in the **Agent's** beneficial ownership occurs or is expected to occur. Company will have thirty days from receiving written notice in which to conduct its own due diligence on the new beneficial owner and determine whether it will continue to do business with **Agent**.

(vii) Neither **Agent** nor any beneficial owner, nor any person or entity acting on **Agent's** behalf is or will become a government entity, government official, a political party, a political candidate or a public international organization without first obtaining the express, written approval of the Company.

(d) In the event that **Agent** fails to perform or breaches any of its agreements in clause (c) or Company does not accept a new beneficial owner as discussed in clause (c)(vii), the Company may, at its sole discretion, rescind this Agreement and **Agent** will pay Company any prepaid fees for products or services that were undelivered at the time of the rescission.

Euronet

Leawood, Kansas, USA
euronet.com

About Euronet

A global leader in payments processing and cross-border transactions, Euronet moves money in all the ways consumers and businesses depend upon. This includes money transfers, credit/debit processing, ATMs, point-of-sale services, branded payments, currency exchange and more. With products and services in approximately 200 countries and territories provided through its own brand and branded business segments, Euronet and its financial technologies and networks make participation in the global economy easier, faster and more secure for everyone.