Whistleblower Policy

Section 1 Overview

1.1 UP Fintech Holding Limited, its subsidiaries, and consolidated affiliated entities (collectively, the "Group" or "UP Fintech Group") are committed to maintaining the highest standards of integrity and honesty in business conduct and financial reporting. This commitment extends to maintaining strict standards pertaining to financial accounting, internal financial controls, auditing processes ("financial matters"), and compliance with applicable legal and regulatory requirements relating to our business in all material respects, as well as strict accordance with the Group's Code of Business Conduct and Ethics (the "Code") and other policies and procedures of the Group.

1.2 The purpose of the Whistleblower Policy (the "Policy") is to provide directors, officers, and employees (collectively, the "Employee" or "Employees") with a process to confidentially report concerns regarding material financial deficiency or fraud, violations of legal and regulatory requirements and violations of the Code (each a "Misconduct") whilst providing protection against retaliation for reports made in good faith. This Policy demonstrates how and where to report a concern, who deals with the report, and how that report will be handled, processed, and documented. This Policy also describes the standards and principles that will govern the processing of all reports no matter whether they are coming from within or outside of the Group.

1.3 In the event that the Group contracts with a third party to handle reports or any part of the report process, the third party should comply with this Policy.

1.4 The Policy is written in English and Chinese languages. In the event of any discrepancy or inconsistency, the English version shall prevail. Employees who have questions as to how the Policy applies should consult the Legal Department or Compliance Department.

Section 2 General Principles

2.1 Confidentiality

The Group, including all persons designated to handle reports under this Policy, will seek to treat all communications as confidential to the fullest extent permitted

under the law and to the extent possible, consistent with the need to conduct an adequate investigation.

2.2 Anonymity

When submitting a report, Employees may do so anonymously. Whilst Employees are encouraged to reveal their identity when submitting a report, as it will make it easier for the Group to address the report, Employees are not required to do so. If an Employee does not reveal his/her identity, the Group will assess the report in the same way as if the identity of the Employee had been provided. However, there may be some practical limitations in conducting an investigation based on anonymous reports.

2.3 Acting in Good Faith

Anyone submitting a report under this Policy must be acting in good faith and having an honest belief that the report is well-founded on a reasonable factual or other basis. Any reports based on allegations that are without solid basis or cannot be substantiated, or that are proven to be intentionally misleading or malicious will be viewed as a serious offense.

2.4 Protection from Retaliation

The Group will provide protection against retaliation for any director, officer, or employee who raises issues or makes a report, in good faith, regarding actual or suspected Misconduct. Retaliation includes any form of penalty or adverse employment consequence, including discharge, suspension, demotion or transfer, harassment or discrimination. Any director, officer, or employee who retaliates against someone who has reported a violation in good faith under this Policy will be subject to various disciplines, including termination of employment. This Policy is intended to encourage and enable officers, directors, employees, and others to raise serious concerns in good faith within the Group for proper resolution.

Section 3 Types of Concern to Be Reported

All directors, officers, and employees have the right and obligation to report concerns in the following areas:

(1) Financial Reporting

examples include: falsification or destruction of business or financial records, misrepresentation or suppression of financial information, non-adherence to internal financial reporting policy/controls, management over-rides, and auditor independence concerns.

(2) Suspected Fraudulent Activity

examples include: theft, defalcation, insider trading, market manipulation, and corrupt practices including giving or receiving bribes or other improper benefits.

(3) Breaches of the Code, Other Compliance Policies and Laws and Regulations

examples include: tax evasion, conflicts of interest, illegal, deceptive, or anti-competitive sales practices, other violations of governing laws and regulations, and non-adherence to the Group's internal compliance policies.

(4) Retaliation or Retribution Against an Individual Who Reports a Concern

examples include: statements, conduct or actions involving terminating, disciplining, demoting, suspending, harassing, intimidating, coercing, or discriminating against an individual who reports a concern in good faith in accordance with this Policy.

Section 4 Report Submission

The Group encourages Employees or external parties to report actual or suspected Misconduct in a timely manner, including breaches of the Code, through one of the channels below. Both reporting options may be adopted on an anonymous basis.

4.1 Email

Please send the report with supporting documents (if any) to ethics@itiger.com.

4.2 By Post

(1) Please send the report with supporting documents (if any) to the below address:

Legal and Compliance Department
9/F, Grandyvic Building, No. 1 Building
No. 16 Taiyanggong Middle Road Chaoyang District, Beijing, China

(2) Please mark "Strictly Private and Confidential – To be Opened by Addressee Only" in a sealed envelope. The report should be addressed to the Compliance Department if it concerns any employees in the Legal Department, and vice versa.

Section 5 Report Handling

5.1 The reports will be reviewed by employees from the Legal Department or the Compliance Department as designated by the Global Chief Compliance Officer (the "Global CCO") (the "Recipient"). Anyone who wants to report a concern about the Global CCO may address such report directly to the Group's CEO. If a report includes Misconduct by an employee from the Legal Department or the Compliance Department, the Global CCO will designate an employee with no direct reporting relationship with the reported employee to conduct an investigation. If a report includes concerns about the Global CCO, the Group's CEO may designate another employee to investigate the report.

5.2 Unless the report has been made anonymously by letter with no contact information, the Recipient should confirm receipt of the communication or report within five business days of receipt.

5.3 The Recipient should register the report in the central log before accessing the report. Both the central log and the report should be kept confidential and secure. If a report is provided by mail or courier in physical format, the Global CCO shall designate at least two employees from the Legal Department and the Compliance Department to open the file on site simultaneously, or the Global CCO may also open the file with another employee from the Legal Department or the Compliance Department on site.

5.4 If the Recipient determines that the report is valid, he or she should conduct the investigation and determine whether further action is required. In conducting his or her investigation, the Recipient may, in consultation with the Global CCO, enlist inside or outside legal, accounting, and human resources employees or other advisors. The Recipient should comply with all rules, regulations and legislation in conducting his or her investigation and should make all reasonable efforts to keep the report and investigation confidential.

5.5 In certain circumstances, the Group may be required to disclose matters relating to material infractions of financial controls, reporting or other matters in accordance with securities laws or stock exchange rules. In such cases the Recipient may be

required to make adequate disclosure in a timely and appropriate manner.

5.6 All investigations should be conducted efficiently, taking into account the nature and complexity of the issues involved.

5.7 On quarterly basis, the Global CCO will report to the Audit Committee and the Group's external auditors the aggregate number of reports received, investigations conducted, and the outcome of those reports and investigations.

5.8 To the extent permitted by law, the Global CCO may inform the whistleblower and/or the person against whom the report has been made of its findings. Any report will remain property of the Group and will not be shared with the whistleblower or any person involving the case.

5.9 The Group may compensate or award the whistleblower based on validity of the report, losses recovered or avoided for the Group, benefits brought to the Group, and other factors.

5.10 Securities laws require the Group to establish procedures for the receipt, retention, and treatment of reports regarding financial matters. This may include reports that are received from third parties. Accordingly, the Global CCO should forward all reports or concerns regarding financial matters received from a third party (including the Group's independent auditor) to the Audit Committee. The Audit Committee should discuss such reports at regularly scheduled meetings (unless they are unfounded or the materiality of the report requires earlier action). The Audit Committee will determine whether a further review or investigation is required and will be free, in their discretion, to consult with any director, officer, or employee to discuss the report and to engage outside experts including auditors, legal counsel or other advisors to assist in the investigation. The results of any further review or investigation shall be documented and reported to the Group’s Board of Directors.

Section 6 Record Keeping

6.1 Any paperwork, recordings, and documents associated with reports are confidential information. Only authorized employees from the Legal Department and the Compliance Department, and outside consultants involved in investigations will be granted access to the report and its associated materials. Any other person is required to get a written pre-approval from the Global CCO before accessing such archives.

6.2 Reports and any investigation conclusions and actions will not be disclosed to any external party unless required by applicable laws or regulations or by any Group policy in place at the time.

6.3 All reports and supplementary documents made through the procedures outlined above are retained by the Legal Department for up to ten years from the date of receipt of such report ("Record Keeping Period").

6.4 After the Record Keeping Period concludes, subject to prior written approval from the Global CCO, such information may be destroyed. However, if such information is relevant to any pending or potential litigation, inquiry or investigation, it should be retained for the duration of such process and thereafter as necessary.