# Unified Fintech Forum: Industry Code of Conduct

April 11, 2025

## TABLE OF CONTENTS

# INDUSTRY CODE OF CONDUCT

## I. INTRODUCTION AND IMPLEMENTATION

In furtherance of Unified Fintech Forum's (formerly Digital Fintech Association of India) ("**UFF**", formerly DLAI) commitment towards creating an industry-led self-regulatory body and aligning its values with the applicable regulatory directions, UFF had first introduced a code of conduct in 2018, which has been updated from time to time. The erstwhile 3rd edition of the code of conduct dated November 30, 2023 is henceforth discontinued and this 4th edition of the code of conduct ("**Code of Conduct**") is instituted in its place. The Code of Conduct will come into effect from April 11, 2025.

Industry self-governance, by virtue of being developed by members of the industry themselves, can lead to more appropriate mechanism for self-regulation with higher compliance rates, better standards of governance, and the safety of customers. Further, self-regulation encourages members to look beyond their immediate short-term goals and internalize the larger impact of their business – such as by deploying customer protection mechanisms, preventing frauds, financial and digital education for customers and employees alike. This leads to a healthier and more profitable ecosystem in the long run. With the recent growth in the fintech industry in India, there is a need for industry participants to adhere to a strong code of conduct to prevent the rise of unscrupulous practices that harm the fintech ecosystem by reducing the confidence of customers, regulators, and other market participants. Safeguarding the interests of customers provides the industry with trust and legitimacy, which will ultimately benefit the fintech industry as a whole and the members individually.

The revised Code of Conduct is centered around 8 (eight) core elements. It sets out the processes and guidelines under each core element to actualize each such element into clear actionable points. This Code of Conduct must be viewed as a minimum industry standard. Consequently, this Code of Conduct is binding on every Member (*defined below*) of UFF, whether such Member is regulated or not. The applicability of this Code of Conduct is set out in Section II *(Applicability)* below.

Each Member of UFF is required to incorporate the Code of Conduct as a part of its fair practices code. This Code of Conduct is required to be displayed by all Members at every point of customer interface – especially on the Member's website and/or mobile application through which it provides its services.

Any concerned person may contact UFF for any queries, information, or clarifications regarding the implementation of the Code of Conduct at: **sro@dlai.in**.

## II. APPLICABILITY

1. In accordance with the articles of association and bye-laws of UFF, UFF has the following categories of members:

   (a) RE Member:

Entities regulated by the RBI, which are permitted to carry out business pertaining to financial products and services, including fintech and digital finance services. ("**RE Member**").

(b) Non-RE Member:

Entities not regulated by the RBI that provide technological solutions for delivery of financial products and services to businesses and consumers or encompass regulatory and supervisory compliance in partnership with traditional financial institutions or otherwise, including entities which facilitate fintech and digital finance related services as a support service i.e., as a lending service provider, fintech platform, technology service provider, data analytics company, etc. ("**Non-RE Member**").

RE Members and Non-RE Members shall collectively be referred to as "**Member(s)**".

In addition to the Members of UFF, the board of directors of UFF also have the right to admit any individual, company, proprietary concern, association, institution, firm, limited liability partnership, body corporate, non-banking financial company, corporation, trust, society, university, government body and self-help group engaged in industry, trade or service and not necessarily engaged in activities relating to fintech sector and the fintech industry, as an 'Associate Partner' which chooses to register and be affiliated with UFF, and participate in events and selected meetings of UFF, without voting rights in the general meeting of Members ("**Associate Partner**").

2. This Code of Conduct is a set of principles, processes, and guidelines that is binding on every Member. Associate Partners are encouraged to voluntarily adopt relevant provisions of this Code of Conduct.

3. Units and functionaries of the UFF Self-Regulatory Organization ("**UFF (SRO)**") referenced in this Code of Conduct shall have the meaning ascribed to them in the table below:

| Units and Functionaries | Meaning |
|---|---|
| Enforcement Committee | The committee established under the UFF (SRO), which shall act as the first forum for reviewing non-compliances by Members, dispute resolution *inter-se* Members and for addressing market threats. |
| SRO Committee | The committee established under the UFF (SRO), which shall act as the appellate forum to the Enforcement Committee for reviewing non-compliances by Members, dispute resolution *inter-se* Members and for addressing market threats. |

4. All Members of UFF are obligated to follow this Code of Conduct. Compliance with the Code of Conduct is a necessary condition for membership. The UFF (SRO) will enforce adherence by Members to the Code of Conduct.

5. Any non-adherence with the measures set out under this Code of Conduct will trigger the governance and enforcement measures set out in clause 7 *(Actions)* of Part H *(Governance and Enforcement)* of Section III *(Code of Conduct)* below.

6. This Code of Conduct aligns with and is in addition to all laws and regulations applicable to entities engaged in the fintech sector, including all current regulations and directions issued by any statutory, regulatory, or governmental body, including, without limitation, the RBI, Securities and Exchange Board of India ("**SEBI**"), Central and State Governments, from time to time and by no means aims to override any applicable law or regulatory guidance. When there is any conflict or inconsistency between this Code of Conduct and any applicable law or regulation in India, such law or regulation will prevail.

   This Code of Conduct is subject to review by the board of directors of UFF from time to time.

## III. CODE OF CONDUCT

### THE CODE OF CONDUCT IS CENTERED AROUND 8 (EIGHT) CORE ELEMENTS:

### A. Transparency and Disclosures

1. Every Member must display the Code of Conduct as part of their fair practices code (if any) at the point of customer interface in English – including on the Member's website (if any) and any mobile application (if any) through which the fintech activities of the Members are undertaken. In addition to English, each Member must ensure that the Code of Conduct is made available or explained in a language understandable by its target customer group, given their geographical and regional location.

2. Members must offer products and services that are not misleading, deceptive, or unclear. Members must ensure that their marketing and advertising material [1] and outreach to customers is not false, misleading, or deceptive.

3. Members must ensure that detailed terms and conditions of the financial products and services offered made available to the customer at the onboarding/ customer engagement stage.

4. RE Members must publish detailed information regarding the fintech products and services offered by them, including, disclaimers regarding risks associated with their products, particulars of customer care, privacy policies, etc. Non-RE Members must provide a link on their website and mobile application to direct customers to the webpage of the concerned regulated entities ("**REs**") they are engaged with.

5. Members must promptly provide UFF (SRO) with all other information that may be required by the UFF (SRO) to ensure compliance with applicable laws, adherence to the Code of Conduct, and promotion of higher standards of governance amongst the Members.

### B. Adherence to Applicable Laws

1. Members must at all times comply with all applicable laws, rules, regulations, guidelines, and circulars promulgated/issued by the government and/or regulatory bodies including the RBI, SEBI, and other relevant authorities.

2. Without prejudice to the generality of paragraph 1 above, Members shall comply with all applicable laws, rules, regulations, and guidelines relevant to their specific area of business in the fintech sector.

   For illustrative purposes:

   - Members operating as payment system operators, payment gateways, and payment aggregators must comply with *inter-alia* the Payment and Settlement Systems Act, 2007, and related rules and regulations, including the 'Guidelines on Regulation of Payment

[1] Members must endeavour to meet any standards on responsible advertising and marketing which may be prescribed by UFF.

Aggregators and Payment Gateways', issued by the RBI on March 17, 2020 (as amended from time to time).

- Members engaged in digital lending activities must adhere to *inter-alia* the 'Guidelines on Digital Lending' issued by the RBI on September 02, 2022 (as amended from time to time).

## C. Fair Interactions

1. Members must ensure that their staff, agents, and representatives are adequately trained to deal with its customers with care and sensitivity, particularly in aspects such as soliciting customers, hours of calling, privacy of customer information and conveying the correct terms and conditions of the products on offer and that their staff, agents and representatives are not rude or humiliating in their dealings with the customer. Members must ensure compliance with the extant RBI guidelines.

2. Members must ensure that there is no undue harassment or intimidation (physical or verbal) of customers, including practices such as calling (or threatening to call) any family member of the customer or any person associated with the customer sending inappropriate messages either on mobile or through social media, making threatening and/ or anonymous calls, etc.

3. Members must refrain from making unsolicited and repetitive telephone calls to customers or prospective customers, including but not limited to, spam calls, robocalls, or other forms of intrusive or harassing communication, and must ensure that all telephone communications with customers or prospective customers are made in a professional and respectful manner.

4. Members must ensure that its customers are not unfairly discriminated against on grounds such as religion, caste, gender, marital status, sexual orientation, etc.

5. Members must ensure that their staff, agents, and representatives use respectful language, maintain decorum, and show respect to social and cultural sensitivities. Further, their staff, agents, and representatives must not contact customers at odd hours or at inappropriate times such as bereavement, illness, or social occasions such as marriages and births.

6. Members must ensure that their staff, agents, and representatives contact their customers only during appropriate hours (between 8:00 a.m. and 7:00 p.m.).

## D. Data Security and Privacy

1. Members must have a board-approved comprehensive data privacy policy compliant with applicable laws, associated regulations and RBI guidelines. Such policy must be disseminated publicly on its website / mobile application and further, at every stage where consent of the customer is taken to access, including collect, process and transfer data of an individual customer, including their personal data.[2] Members, in their capacity as a data fiduciary, must provide a notice in such privacy policy, in clear and plain language, informing customers of, *inter-alia*:

[2] Here, "personal data" means any data about an individual who is identifiable by or in relation to such data.

(a) the personal data sought to be collected,

(b) the purpose of processing personal data,

(c) the manner in which the customer may withdraw the consent given to the Member to process their personal data, seek grievance redressal, make a complaint to the Data Protection Board ("**DPB**"),

(d) the type of data that can be stored,

(e) the length of time for which data can be stored,

(f) restrictions on the use of data, data destruction protocol, standards for handling security breaches, and

(g) the details of third parties (if any) who are allowed to collect personal data of the customers through such Member.

2. The customer should be provided with the option to access the privacy policy in English, or in any other Indian language mentioned in the Constitution of India. The privacy policy must include the contact details of a 'Data Protection Officer', or of the person authorized by the Member, to respond to any communication from customers to exercise their rights under the Digital Personal Data Protection Act, 2023 (as amended from time to time) ("**DPDP Act**").

3. If the customer has given their consent to the processing of their personal data before the commencement of the DPDP Act, then the Member must, as soon as reasonably practicable, give the customer a fresh notice of the personal data that was processed, the purpose for processing, the manner in which the customer may now withdraw consent that was previously provided and seek grievance redressal, etc.

4. Members must follow a consent-based architecture for accessing data (including collecting and processing personal data), with the prior and explicit consent of customers. In respect of collecting and processing personal data, Members must obtain the free, specific, informed consent of customers through an unambiguous indication, i.e., a clear affirmative action. Members must provide customers with the option to give or deny consent for use of specific personal data, restrict disclosure of data to third parties, data retention or make the application delete or forget the data. The Member shall preserve such digital records of customer consent(s) as proof of informed consent.

5. Members are required to practice good faith in the collection, storage, use, and sharing of personal data of customers in respect of their fintech related activities.

6. Without limiting the generality of the above, Members shall not:

(a) intentionally request personal data from a customer even though there is no service that can be provided to a customer;

(b) intentionally collect personal data that is not relevant to the services that will be provided to the customer by the Member;

(c) collect personal data outside the data that has been agreed to be given by the customer;

(d) use and/or process personal data for purposes that have not been notified or purposes that are different from what was previously notified to the customer;

(e) collect, process and/or store customers' personal data even though the Member or any person authorized by the Member to collect, process or store such personal data does not yet have a reliable system or processes to carry out such activities in accordance with applicable data protection laws;

(f) share personal data of customers with third parties without explicit consent from the customer;

(g) share such personal data with third parties other than for purposes consented to by the customer or where it is required under applicable law;

(h) use a customer's mobile phone resources like file and media, contact list, call logs, telephony functions, etc.;[3]

(i) use the personal data in any manner which is likely to cause physical harm or injury to any customer, their family member, or any person associated with the customer; and

(j) refuse to provide any fintech related products or services or any related support services, solely on account of a customer denying or withdrawing their consent for collecting, processing or storing any of their personal data which is not necessary for the provision of such products or services by the Member.

7. Members may access, collect, process and store personal data of its customers in respect of their fintech activities, provided that:

(a) the Member is responsible for data protection compliances in respect of any personal data processed by the Member itself. In case the Member engages a third-party service provider for processing the personal data on its behalf, the Member must ensure compliance by the third party processor through its data processing agreement.

(b) the Member can justify that a certain data set is needed in connection with its operations or to perform a certain function for and on behalf of the associated RE (under the terms of its partnership agreement).

(c) if such Member is engaged in digital lending, the Member can demonstrate a tangible and direct link between the borrower data collected and the economic profiling of the borrower enabling credit decision-making by it or by the associate RE. Such credit decision-making rationale must be auditable.

[3] This does not include the one-time access, with the explicit consent of the customer, that can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/KYC requirements.

(d) the data is collected with the explicit consent of the customer. Such customer consents must be recorded by the Member in a manner that is auditable.

(e) the Member ensures that the customer can withdraw their consent for the collection and processing of their personal data at any time through simple and easy means. On withdrawal of their consent, the Member must – within a reasonable time – cease the processing of the customer's personal data (except if required by law to do so).

(f) the user interface of the mobile application and/or website of a Member must not facilitate 'umbrella consent' or 'consent fatigue'. Instead, the Member must obtain free, specific, informed and unambiguous consent of customers through a clear affirmative action.

(g) the Member shall ensure that the customer is clearly made aware of the data points that will be accessed and the personal data that will be collected and processed. The Member must obtain upfront consent of its customers for the collection, processing, storage, utilization, and sharing of any customer information.

(h) Members must not obtain over-arching access to a customer's mobile phone resources like files and media, contact list, call logs, or telephony functions. Any such access must be strictly need-based and related to the products or services proposed to be provided to the customers.

(i) the purpose of the collection of personal data and taking the consent of the customer is clearly disclosed by the Member to the customer at each stage of personal data collection.

(j) the customer is given the option to both give and deny consent for the use of specific data, restrict disclosure of such data to third parties by Member, withdraw previously granted consent to access personal data, limit the time period for which such data can be stored by the Member and require the Member to delete the data collected from the customer.

(k) the Member must inform the customer of and give effect to various rights they are entitled to in respect of their personal data, including their rights to:

  (i) access information about their personal data;

  (ii) correct, complete, update and erase their personal data; and

  (iii) obtain grievance redressal.

(l) The Member must undertake reasonable efforts to ensure that personal data of customers processed by it is accurate and complete, if the personal data is likely to be used to make a decision about customers or disclosed to a third-party data fiduciary.

(m) the personal data collected is only processed and used for the limited purposes, as disclosed to the customer.

(n) only minimal personal data, which is critical for the Member to carry out its operations and functions or as required by the associated RE under the terms of the partnership arrangement (as applicable), must be stored by the Member.

(o) The Member must cease to retain any personal data of customers and erase such personal data as soon as it is reasonable to assume that:

(i) the purpose for which the personal data was collected is no longer being served;

(ii) the customer has withdrawn their consent to process personal data; or

(iii) retaining the personal data is no longer necessary for legal purposes.

(p) the Member shall not store any biometric information of any customer, other than as permitted under extant statutory guidelines.

(q) all data collected by the Member is stored only on servers located in India.

(r) the Member shall implement appropriate technical and organisational measures to ensure effective protection of the personal data of customers by taking reasonable security safeguards to prevent personal data breach and the technology deployed by the Member shall comply with the technology standards/ requirements on cybersecurity stipulated by the RBI and other agencies, from time to time, for undertaking its fintech activities.[4]

(s) In the event of a personal data breach, the Member shall notify the DPB and each affected customer in the form and manner as specified by the DPB, of such breach.

(t) Members may, in the capacity of the agent of the customer, seek the credit information of the customer from the credit information companies, by providing satisfactory identification along with the consent of the customer to obtain such information on the customer's behalf.

## E. Customer Grievance Redressal

1. Each Member should have a board-approved policy for addressing customer complaints in a fair, and prompt manner covering the process to register, resolve and escalate the complaints, internal and external escalation mechanism, turnaround time, complaint categories, review/audit of redressal system, and reporting to the board and top management. Each Member shall put into place an efficient mechanism for the implementation of such customer complaint policy and for the resolution of customer complaints in compliance with the contractual and statutory rights of the customer.

2. Each Member must appoint a suitable nodal grievance redressal officer to oversee the customer grievance redressal function. Every Member must prominently display the contact

[4] Here, "personal data breach" means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

details of such nodal grievance redressal officer and the customer grievance redressal mechanism on their website, mobile application and other points of customer interface.

3. Each Member shall provide to customers, including by publishing on its website, details of how the customer can contact customer service / concerned compliance officer at the Member or seek redressal of customer complaints. Each non-RE Member should also provide details of how customers can contact the REs, which are involved in providing the relevant financial product or services to the customer.

4. Each Member must also publicize the following details of the customer grievance redressal mechanism set up by UFF:

   - UFF's email ID for customer grievances: cgrm@dlai.in

5. Members should provide details in respect of the right of a customer to raise complaints in consumer forums, under the Reserve Bank-Integrated Ombudsman Scheme (**"RBI Ombudsman"**), RBI's Sachet Portal, etc. (as applicable) and guidance on how a customer can approach such authorities.

6. Members engaged in digital lending must have a mechanism as part of their grievance redressal framework for the redressal of recovery-related grievances, the details of which must be provided to the customer in the key fact statement. It shall be sufficient compliance if the Member can re-structure/re-organize its existing redressal system to identify and promptly address recovery-related grievances.

7. Members must record and analyse individual and aggregate level data for the grievance redressal system capturing the nature of complaints, action taken, and turn-around time. Report on grievances received, resolved, and pending along with the nature of complaints should be reported quarterly to UFF within 15 (fifteen) days of the end of each quarter.[5] Members are also encouraged to present the same before their boards as a good governance practice.

## F. Employee Training

1. Members must give comprehensive induction training to the employees on policies, processes, and regulations. Emphasis should be given to Code of Conduct-related aspects on customer-interface aspects such as fair treatment, the privacy of data, service quality, customer grievance redressal system, prevention of sexual harassment, relationship management, conveying the correct terms and conditions of the products on offer, assessing repayment capacity of a customer, dealing with difficulty in repayment, performance, and recovery targets etc.

2. Members must regularly assess employees' understanding of the elements noted above and conduct refresher training to address the gaps in understanding.

[5] This quarterly reporting must be done as per the format prescribed by UFF in this regard.

3. Members must train their employees on understanding and dealing with gender issues including appropriate interaction with women or trans colleagues and customers.

4. Members must necessarily orient their employees on professional conduct and integrity issues including expected behaviour and non-indulgence in any unlawful and anti-social activities.

5. Members must engage new employees in the business operations who will have direct interface with customers only after completion of their induction training.

6. Members must ensure that employees directly responsible for the grievance redressal system receive detailed training about the system, processes, and soft skills required for resolving complaints.

7. Members engaged in digital lending must ensure that the compensation matrix for the recovery staff should not solely be dependent on the quantum of recovery by an individual, and rather, it must be designed in a manner to align their behaviour with fair interaction practices as mentioned in Part C *(Fair Interaction)* of this Section III of this Code of Conduct.

## G. Customer Awareness

1. Each Member must take measures to ensure that customer fully understand the products, process, and terms of the contract. Such measures must be provided to the customers free of cost.

2. Each Member must provide a receipt/acknowledgement for every payment, including the digital payments, received from the customer.

## H. Governance and Enforcement

1. Each Member is obligated to adhere to all applicable regulations in letter and spirit.

2. Each Member will comply with all provisions of all applicable laws and regulations, including, but not limited to:

   (a) Applicable laws and regulations concerning financial services and consumer protection, including without limitation all directions, guidelines, circulars, and notifications issued by RBI and other relevant statutory, regulatory, or government bodies;

   (b) Applicable laws and regulations in the field of communication and informatics related to the protection of personal data in electronic systems; and

   (c) Any other applicable law and regulations relating to business, operations, and practices of such Member.

3. All provisions in this Code of Conduct are complementary and in addition to the obligations of each Member under laws and regulations applicable to the Member. Each Member is individually and solely responsible for its compliance with applicable laws, regulations, and this Code of Conduct.

4. Obligation to adhere to this Code of Conduct

(a) At the time of availing membership with UFF, the Members must affirm in writing to adhere to the Code of Conduct.

*Provided that* existing Members must within 1 (one) month from the date on which this Code of Conduct becomes effective, affirm in writing to adhere to the Code of Conduct.

(b) At the time of renewal of membership with UFF, the Members must affirm in writing to adhere to the Code of Conduct.

(c) Each Member will nominate a designated officer from within their organisation who will be the point of contact for all correspondence (including reporting) with UFF ("**Designated Officer**"). The name and correspondence details of the Designated Officer must be intimated to UFF immediately upon nomination, and in any case, not later than 3 (three) days.

(d) Each Member shall follow advisories/directives any other communication of sectoral importance, issued from time to time by UFF.

(e) Each Member institution shall share with UFF, the data and information requested from time to time for sectoral publications, research and/or as may be required by any government agency or applicable law.

(f) The Designated Officer must ensure that the fair practices code of the Member (which incorporates this Code of Conduct) is disseminated within the organization of the Member after any update to this Code of Conduct and in any case, at least once every calendar year.

5. Reporting

(a) Ad-hoc:

(i) In the event of any non-adherence by a Member of the Code of Conduct or any applicable law, such Member may voluntarily self-report such non-compliance to the UFF (SRO) immediately and in any case within 7 (seven) business days of such non-adherence.

(ii) In the event of the occurrence of any cyber security incidents[6] affecting any Member, such Member must (and in any case within 6 (six) hours of noticing such incidents or being brought to notice about such incidents) report such incidents to Cert-In, the RBI and the UFF (SRO) secretariat.

[6] Here, "cyber security incidents" means the types of cyber security incidents identified in Annexure I of the Cyber Security Directions dated April 28, 2022, notified by the Indian Computer Emergency Response Team ("**Cert-In**") under the Ministry of Electronics and Information Technology and as further explained by the FAQs released by Cert-In. Reporting of such cyber security incidents to Cert-In. Reporting may be done via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). Other incidents may, at the option of the Member, be brought to the notice of UFF, the RBI and Cert-In.

(b) Quarterly:

Each Member must record and analyse individual and aggregate level data for a grievance redressal system capturing the nature of complaints, action taken, and turn-around time. Report on grievances received, resolved, and pending along with the nature of complaints should be reported on a quarterly basis to the CGRM Unit of UFF, within 15 (fifteen) days from the end of each quarter.[7]

(c) Annually:

Each Member must submit an annual confirmation to the UFF (SRO), in writing, on its compliance with the Code of Conduct, in such form as the UFF (SRO) may require from time to time (**"Annual Submission"**). The Annual Submission will include a certification by a director, company secretary, or other key managerial personnel of the Member that it is in compliance with the Code of Conduct and other applicable laws/regulations. The Annual Submission will be required from each Member to continue their membership and participation in UFF activities.

6. Dispute Resolution

(a) The dispute resolution mechanism prescribed under this clause 6 will only apply to disputes inter se Members in respect of the interpretation, applicability or any other aspect relating to this Code of Conduct or in respect of the terms and conditions of their membership to UFF.

(b) Consultation:

(i) Members hereby agree to first afford adequate opportunity for bilateral consultation regarding any representations made by another Member.

(ii) If a request for consultation is made, the Member to which the request is made shall, unless otherwise mutually agreed, reply to the request within 10 (ten) working days after the date of its receipt and shall enter into consultations in good faith within a period of no more than 30 (thirty) days after the date of receipt of the request, with a view to reaching a mutually satisfactory solution.

(iii) If the Member does not respond within 10 (ten) working days after the date of receipt of the request or does not enter into consultations within a period of no more than 30 (thirty) days, or a period otherwise mutually agreed, after the date of receipt of the request, then the Member that made the initial request for consultation may proceed directly to request the Enforcement Committee to decide such matters.

(iv) Consultations shall be confidential, and without prejudice to the rights of any Member in any further proceedings.

[7] This quarterly reporting must be done as per the format prescribed by UFF in this regard.

(c) Enforcement Committee:

(i) If the consultations fail to settle a dispute within 60 (sixty) days after the date of receipt of the request for consultations, the dispute will be decided by the Enforcement Committee. The Enforcement Committee will notify a fair procedure for the settlement of disputes inter-se Members.

(ii) If any Member is aggrieved by the decision of the Enforcement Committee, an appeal may be filed before the SRO Committee, which must act in consultation with the board. The SRO Committee will notify the timelines for filing such appeals and a fair procedure for settlement of disputes inter se Members. The decision of the SRO Committee shall be final and binding on the Members.

7. Actions

(a) The UFF (SRO) will monitor compliance with the Code of Conduct by Members. Additionally, an anonymous peer complaints system will also be set up by UFF whereby Members can bring forth instances of non-adherence (details to be submitted with evidence to UFF) with the Code of Conduct or applicable law by other Members to the notice of UFF.[8]

(b) The Enforcement Committee will notify a fair procedure for the admission of complaints against any Member for the violation of the Code of Conduct, investigation, and determination of a violation of the Code of Conduct, and the decision on an application of Actions (*defined below*) against the non-compliant Member after giving reasonable opportunity to such Member to make representations in such a process.

(c) Any decision taken by the Enforcement Committee on non-compliance with the Code of Conduct will be binding on the relevant Member but will be subject to an appeal to the SRO Committee. The decision of SRO Committee will be final and binding.

(d) The Enforcement Committee will be entitled to take the following actions ("**Actions**") for non-compliance by a Member with the Code of Conduct or other applicable law, after providing an opportunity of hearing to such Member(s), and while the non-compliance still persists:

(i) issue warning letter(s) to a Member;

(ii) bar the non-compliant Member from future membership of UFF, participating in its events, and/or from forming part of the board or any of the committees of UFF for such a period of time as the Enforcement Committee may deem fit;

(iii) notify all other Members of the abeyance of the membership and debarment of the non-compliant Member, and to also publish the fact of such abeyance and debarment in a 'grey list of non-compliant fintech entities' maintained by UFF in its records which may or may not be publicly available. This grey list will

[8] Members of UFF can highlight non-compliance by other Members via email at sro@dlai.in. Any such peer reporting would be anonymous, and the name of the complainant will not be, in any case, disclosed to the non-compliant Member.

be revised periodically by the UFF (SRO) acting in accordance with the directions of the Enforcement Committee. The placement of the Member in the grey list will be seen as having an adverse impact on the reputation of such Members;

(iv) upon receiving a formal request from an entity placed in the grey list, such grey list will be reviewed periodically by the Enforcement Committee of UFF and those entities which are in the list, if demonstrate compliance to the satisfaction of Enforcement Committee & SRO Committee, may be removed from the list after 3 (three) months, with the approval of SRO Committee on case-to-case basis;

(v) report any serious violation of the Code of Conduct to the appropriate authorities, including the RBI;

(vi) pass such other directions as the SRO Committee upon recommendation of the Enforcement Committee may consider fit for ensuring compliance with the Code of Conduct, including obtaining a binding commitment from the Member to take necessary remedial steps for compliance with the Code of Conduct; and

(vii) may terminate their membership with UFF, after an adequate opportunity has been given to the Member to rectify such non-compliance. At least 2 (two) written warning letter(s) shall have been issued by UFF to such Member prior to cancellation of membership.

(e) Within 21 (twenty-one) days of receipt of the decision of the Enforcement Committee, the managing director of the Member may: (i) duly acknowledge the Enforcement Committee's action with a commitment letter; or (ii) appeal to the SRO Committee in accordance with clause 8 *(Appeal)* below. The commitment letter must outline the corrective steps which the Member proposes and undertakes to fulfil, to remedy the non-adherence to the Code of Conduct. The Member must also commit to undertake required steps to prevent (to the extent reasonably practicable) to address the occurrence of such non-compliance in the future (except due to factors beyond its control/ *force majeure*). Evidence of corrective action, wherever necessary, must also be taken from the Member.

Provided that the Actions above may be vacated by the Enforcement Committee if within 21 (twenty-one) days of receipt of the decision of the Enforcement Committee, the non-adherence, and its consequences are, in the opinion of the Enforcement Committee, remedied pursuant to such corrective action.

(f) If no response is received from the managing director of the Member within 21 (twenty-one) days of receipt of the decision of the Enforcement Committee, the matter must be reported to the SRO Committee for further action, which may include reporting to RBI by UFF (SRO).

(g) The Enforcement Committee shall consider the following parameters in its decision:

(i) the regulatory and industry standards violated.

(ii) the impact on customer interests.

(iii) the systemic impact of such violation on the industry.

(iv) the nature of the violation (procedural/policy, severity, magnitude, first-time/repeat);

(v) the response of the Member, including whether the Member self-reported such non-compliance;

(vi) age and size of the Member and duration of membership with UFF to determine if the lapse is due to limited capacities and resources; and

(vii) any other factor that the Enforcement Committee considers relevant.

8. Appeal

(a) If the Member is aggrieved by the decision of the Enforcement Committee, an appeal may be filed before the SRO Committee, within 21 (twenty-one) days from the date of receipt of the communication from UFF (SRO) regarding the decision of the Enforcement Committee.

(b) If no appeal is filed within the above period, the order of the Enforcement Committee shall attain finality.

(c) The decision of the SRO Committee taken in appeal will be final and binding on the Member. The SRO Committee can levy any Actions and must take into account the factors mention in sub-clause (g) of clause 7 *(Actions)* above, in its decision.

Our website: www.dlai.in

Any questions regarding this code of conduct can be sent to UFF at sro@dlai.in