Draft SAFER Standards for NFT Marketplaces

1. Preliminary & Context

This is a voluntary standard to enhance consumer trust and safety on Non-Fungible Token (NFT) marketplaces. The scope of these standards extends to NFT marketplaces dealing in the transfer of NFTs linked to intangible assets.

NFTs are unique digital identifiers relied on to certify ownership and authenticity. They provide a means of creating traceable titles for intangibles. Thus, NFTs are considered an important technological development for IP industries. Indeed, many of the highest valued NFTs are linked to digital art. At the same time, NFT marketplaces are notorious for widespread IP theft. In addition, a majority of these marketplaces place considerable responsibility on the consumer to verify the legitimacy and authenticity of NFTs sold on their platforms, something that is incredibly difficult to do with digital goods. These platforms also offer consumers little to no recourse, legal or otherwise, in the event of any loss. The Consumer Protection Act, 2019 should apply to NFT marketplaces, as its definition of e-commerce includes the "buying or selling of … digital products over a digital or electronic network".[1] However, there remains some ambiguity around the application of the Consumer Protection Act to NFT marketplaces as the term "digital products" is not defined. As such, many NFT marketplaces are "Buyer Beware" ecosystems. The term "Buyer Beware" denotes a commercial environment characterised by limited consumer confidence because contracts of sale are typically one-sided and exclude important consumer rights in transactions.

NFT marketplaces are distinct from traditional e-commerce platforms as the latter sell physical goods whereas the former deal primarily in intangibles. However, as alluded to before, these marketplaces are still a form of e-commerce. India requires traditional e-commerce companies to comply with the Legal Metrology Act, 2009, which establishes and enforces standards of weights and measures and regulates trade and commerce in goods that are sold or distributed by weight, measure or number. The Legal Metrology Act sets a standard to ensure uniformity of quality and experience in the purchase of physical goods. However, the concept of weights and measures cannot apply to digital goods. Additionally, it may not be advisable to establish standards for these products in the infancy of their technological development.

There is, however, no practical impediment to standardise the information available about NFTs on the platforms they are sold on. Indeed, creating a standard for information about NFTs would help consumers better navigate marketplaces by enabling them to make informed choices about their purchases.

Policymakers in India have now started paying attention to NFTs. In 2022, the Ministry of Finance issued a tax scheme for virtual digital assets, which would include NFTs notified or designated by the Government. In the same year, the Central Board of Direct Taxes clarified that NFTs linked

[1] Section 2(16) of the Consumer Protection Act 2019.

to intangible assets would come under the definition of VDAs for taxation purposes.[2] In March 2023, the Department of Revenue issued a notification clarifying that entities engaged in VDA-related activities were required to comply with the Prevention of Money Laundering Act, 2002. However, there are currently no frameworks that tackle the issue of consumer trust and safety in NFT marketplaces in the country.

In this context, the ETCI has put together a set of information standards for NFT marketplaces to engender greater trust and safety for consumers in these ecosystems.

2. Introduction to the SAFER Standards

The Safety from **H**arm through **A**wareness, **F**ortification, and **E**ffective **R**edressal of complaints (SAFER) Standards aim to equip consumers with tools to make better and more informed choices when purchasing or investing in NFTs. To this end, the standards emphasise informing consumers through labels. Labels are more easily understood by a wider variety of stakeholders and are less time consuming to read than other forms of notification. Labels also help accommodate an abundance of information in a limited space.

Labelling has a long and effective tradition in policy promotion. Perhaps the most famous illustration of a voluntary labelling program deployed to promote policy goals is Energy Star. The Energy Star program was launched in 1992 by the US Environmental Protection Agency to identify and promote energy-efficient products.[3] The program has helped consumers save USD 430 billion on their utility bills and reduced the carbon footprint of household appliances by 2.7 billion metric tons of carbon dioxide since its inception. In addition, the Energy Star enjoys 90 percent brand recognition.

Labelling has potential for positive impact in technology sectors as well. Internationally recognised bodies like the National Institute of Standards and Technology (NIST) have advocated labelling as an approach to promote consumer safety and security in the IoT sector.[4]

Inspired by the success of labelling as a consumer-friendly tool for communicating important information, the SAFER standards suggest the usage of "binary" labels, that specify whether a product does or does not meet the required criteria. The premise behind binary labelling is to accommodate businesses that may not have the means to authenticate the NFTs or verify sellers on their platforms. Binary labelling allows such businesses to indicate that the condition has not been met i.e. a particular product or seller is not verified. Such labels can be incorporated in the user interface of the NFT marketplace.

[2] NFTs linked to tangible assets whose transfer is legally enforceable would not fall under this definition.
[3] https://www.osti.gov/servlets/purl/806113
[4] See generally: Consumer Cybersecurity Labeling for IoT Products, https://www.nist.gov/system/files/documents/2021/12/03/FINAL_Consumer_IoT_Label_Discussion_Paper_20211202.pdf.

In addition to the focus on labels, the standards set out here are grounded in existing legal requirements for e-commerce marketplaces in India as well as global best practices applicable to NFT marketplaces. For more information on our methodology, please click here.

The application of these standards will potentially benefit all stakeholders in the ecosystem. Consumers will gain from reduced information asymmetries and be less vulnerable to fraudulent activities. Industry will benefit from increased consumer confidence and a set of rules for the road on how to mitigate harms on their platform. Finally, decision-makers will benefit from a consumer protection standard that reduces consumer complaints and prevents several public interest concerns emanating from NFT marketplaces.

3. SAFER Trust and Safety Standards for NFT Marketplaces

3.1. Definitions:

The following terms have been used in the standard:

a) **Advertisement**: The term "advertisement" means any audio or visual publicity, representation, endorsement or pronouncement made by means of light, sound, smoke, gas, print, electronic media, internet or website and includes any notice, circular, label, wrapper, invoice or such other documents.[5]
b) **Age gating**: An age gate is an age verification system in which a technical measure (like a website pop-up) is used to ask users to confirm their age. Those who are underage will not be allowed to access digital content.
c) **Attribute Indicators**: Attribute indicators are symbols, logos, buttons or other aspects of an NFT marketplace's user interface that indicate particular properties or feature of NFTs. Examples of such attributes are whether the NFT includes copyright over the underlying work, and whether the NFT is distinct or a part of a large collection.[6]
d) **Clear and Understandable Language**: Language that is clear, concise, well-organized, and follows other best practices appropriate to the subject or field and intended audience.[7]
e) **Consumer**: A consumer is an individual member of the general public who is the end user of products and services (which might not be the customer who purchased the product or service.[8]
f) **Copyright**: Copyright is a bundle of rights given by the law to creators of literary, dramatic, musical and artistic works and producers of cinematograph films and sound recordings. These include (depending on the nature of the work), *inter alia,* rights of reproduction, communication to the public, adaptation and translation of the work.[9]

[5] As per Section 2(7) of the Consumer Protection Act, 2019.
[6] These properties can be defined by the respective NFT marketplace. For example, OpenSea uses a metric called OpenRarity (https://www.openrarity.dev) that gives a "transparent, mathematically sound rarity calculation that is entirely open-source and reproducible by anyone".
[7] Adapted from the Plain Writing Act, 2010, available at https://www.govinfo.gov/app/details/PLAW-111publ274.
[8] This definition is in line with the ISO standards on Customer Satisfaction Section 3.3; adapted from https://www.iso.org/obp/ui/#iso:std:iso:10008:ed-2:v1:en
[9] Adapted from the Handbook on Copyright Law, available at https://copyright.gov.in/documents/handbook.html.

g) **Harm**: The harm or loss that consumers experience which is not linked to consumer misjudgement or regret, when, for example, i) they are misled by unfair market practices into making purchases of goods or services that they would not have otherwise made; ii) they pay more than what they would have, had they been better informed, iii) they suffer from unfair contract terms or iv) the goods and services that they purchase do not conform to their expectations with respect to delivery or performance. Consumer harm can be structural in nature (i.e. affecting all consumers) or personal; apparent to consumers or hidden; financial or non-financial. Consumer detriment may be apparent to consumers immediately, may take time to emerge, or remain hidden.[10]

h) **Marketplace Vulnerabilities**: A marketplace vulnerability is an underlying issue with an NFT marketplace that could leave its users susceptible to fraud, theft, or other loss. This could take the form of weakened cyber-security of the NFT platform.[11]

i) **Non-Fungible Tokens**: Non-Fungible Tokens (NFTs) are digital crypto assets with a unique digital identifier for ownership, powered by blockchain technology, which cannot be interchanged with others. NFTs usually refer to digital items that can be easily reproduced such as, images, text, audio, video etc. and that are in practice used as collectibles rather than as payment or investment instruments.[12]

j) **NFT marketplace**: A NFT marketplace is any legal or natural person or entity that carries out the following activities, namely[13]:

- exchange between non-fungible tokens and fiat currencies;
- exchange between one or more forms of non-fungible tokens or virtual digital assets;
- transfer of non-fungible tokens;
- safekeeping or administration of non-fungible tokens or instruments enabling control over non-fungible tokens.

k) **Personally Identifiable Information**: Personally Identifiable Information is any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, can identify such person.[14]

l) **Smart contract Vulnerabilities**: Smart contract vulnerabilities are issues with the smart contracts that underpin NFT ownership and tracking. They can arise from errors in high level code, hacking of public smart contracts by malicious actors, structural problems with smart contracts, amongst others.[15]

---

[10] Adapted from the OECD Recommendation on Consumer Policy Decision Making, available at https://one.oecd.org/document/DSTI/CP(2019)13/FINAL/En/pdf.
[11] Adapted from: https://www.blockchainx.tech/nft-vulnerability-and-security.
[12] Adapted from Updated-Guidance-VA-VASP.pdf - FATFhttps://www.fatf-gafi.org › recommendations and https://arxiv.org/pdf/2210.14942.pdf.
[13] Adapted from https://archive.gazettes.africa/archive/za/2022/za-government-gazette-dated-2022-11-29-no-47596.pdf
[14] Adapted from the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[15] Adapted from "Understanding Security Issues in the NFT Ecosystem", available at https://arxiv.org/pdf/2111.08893.pdf.

m) **Trademark**: A trademark is a mark that can be represented graphically and can distinguish the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours.[16]

n) **User Interface**: User Interface (UI) is defined as the way a person interacts and commands a computer, tablet, smartphone, or other electronic device. UI comprises the screen menus and icons, keyboard shortcuts, mouse and gesture movements, command language and online help.[17]

o) **Virtual Digital Assets**: Virtual Digital Assets (VDAs) are any information or code or number or token (not being Indian currency or foreign currency), generated through cryptographic means or otherwise, by whatever name called, providing a digital representation of value exchanged with or without consideration, with the promise or representation of having inherent value, or functions as a store of value or a unit of account including its use in any financial transaction or investment, but not limited to investment scheme; and can be transferred, stored or traded electronically.[18] NFTs have been included in the definition of VDAs, though their exact definition has been left to the Central Government to notify.[19]

p) **Vulnerabilities**: Vulnerabilities are systemic technical weaknesses that may be exploited by hackers for unlawful gains at the expense of the platform or the consumer. They may affect the platform wallet which is used to store the digital works of the users; they can arise due to cyber-attacks in the marketplace itself; or they may affect the smart contracts that govern the blockchain behind the NFT marketplace.

q) **Wallet Vulnerabilities**: A wallet vulnerability arises when a platform's wallet, which is used to store a user's digital assets like NFTs and cryptocurrency, is broken into by attackers. It can be seen as a subset of market vulnerability.[20]

r) **Work**: A work is defined as a literary, dramatic, musical, or artistic work, a film, or a sound recording. Artistic works mean a painting, a sculpture, a drawing (including a diagram, map, chart, or plan), an engraving or a photograph, a work of architecture or any other piece of craftsmanship – regardless of the fact that such work possesses artistic quality.[21]

[16] As defined in Section 2(1)(zb) of the Trademark Act, 1999.
[17] Adapted from https://www.pcmag.com/encyclopedia/term/user-interface.
[18] Section 2(47A) of the Income Tax Act 1961 (as introduced by the Finance Bill in 2022).
[19] Explanation (a) to Section 2(47A) of the Income Tax Act 1961.
[20] Adapted from "Identifying Security Risks in NFT Platforms", available at https://arxiv.org/pdf/2204.01487.pdf.
[21] Adapted from Section 2(c) and Section 2(y) of the Copyright Act, 1957.

4.2 The ETCI proposes the SAFER Standards for engendering greater trust and safety in NFT Marketplaces:

Safety from Harm through Awareness: Several consumer harms on NFT marketplaces arise due to information asymmetries about sellers and NFTs. NFT marketplaces should, therefore, take steps to safeguard users from such harms. This should be done by equipping the consumer with enough information to have awareness and understanding about an NFT transaction. To that end:

- **Protection of Children's Interests**: NFT marketplaces should:
  - ensure age-gating at the time of sign-up so that users under the age of 13 are not transacting on the platform.
  - For any minor between the ages of 13 and 18, establish accounts with the consent of the parental guardian. This can be clubbed with consent obtained under the Digital Personal Data Protection Bill, when enacted.
  - In case of any suspicious or abnormal activity related to the minor account, the parental guardian must be notified immediately.

- **Seller Verification**: NFT marketplaces should:
  - create a program for seller verification.
  - install a system of seller verification based on a seller's verifiable Personal Identification Information (PII). The requirement for supply such PII can be premised on a threshold for spending i.e., if a user spends more than a certain amount on an NFT the seller has to provide PII for the transaction to go through.
  - clearly indicate the liability of sellers (verified and unverified) in their policies.
  - use a label to indicate whether a seller is verified or unverified (indicative illustration below).

Seller Verified

Seller Not Verified

Disclaimer: Labels should not confuse consumers with jargon and should cover explicit and implicit claims about products.

- **Seller Rating System**: NFT marketplaces should include a seller rating system. Additionally they should:
    - indicate feedback from verified purchasers about seller quality.
    - make best efforts to ensure that the feedback mechanism is in line with the Bureau of Indian Standards' IS 19000:2022 on 'Online Consumer Reviews – Principles and Requirements for their Collection, Moderation and Publication'.[22]
- **Legitimate Content with Unambiguous Attributes**: NFTs sold on NFT marketplaces may or may not be infringing the intellectual property rights of other works – which in turn might harm the interests of the NFT purchaser. To that end, NFT marketplaces should:
    - require sellers to provide undertakings about the veracity and accuracy of the products they are selling.
    - provide attribute indicators for each work sold through a prominently displayed label on aspects such as IP in work underlying the NFT, restrictions on how the NFT can be used (for example: the NFT cannot be transferred out of the NFT marketplace to the user's personal wallet) etc. Illustrative example:

Seller Owns Rights to Material in NFT

Seller May Not Own Rights to Material in NFT

Disclaimer: Labels should not confuse consumers with jargon and should cover explicit and implicit claims about products.

- **Accountable and Responsible Advertisements**: NFT Marketplaces should:
    - *not* engage in deceptive or misleading advertisements (that is, where a misrepresentation, omission, or practice is likely to mislead a consumer).[23]
    - ensure that their advertisements carry disclaimers to make consumers aware of the risks of investing in digital assets.
    - ensure their briefs to celebrities/influencers who are promoting them disclose any material connection to the marketplace and be able to substantiate any claims that are being in the advertising material.

- **Fair Trade Practices:** NFT Marketplaces should:
    - *not* adopt any unfair trade practices and should make best efforts to ensure that transactions on the platform are non-fraudulent and consumer-friendly.

[22] This standard is applicable to any organisation that publishes consumer reviews online, including suppliers/sellers of products and services that collect reviews from their own customers, a third-party contracted by the suppliers/sellers or an independent third party. Available at https://www.medianama.com/wp-content/uploads/2022/12/19000_2022.pdf.
[23] Adapted from https://ca.practicallaw.thomsonreuters.com/w-030-4989?transitionType=Default&contextData=(sc.Default)&firstPage=true

- make clear disclosures about conflicts of interest.
- be transparent about pricing and fees. These details should be made available in clear and understandable language available easily on their pages.
- indicate a NFT's purchase price and transaction history clearly in their User Interface.

Fortification: Like any digital platform, NFT marketplaces are also susceptible to attacks. If adequate attention is not paid to cyber-security, users harm ensues. There are several examples of platform vulnerabilities that lead to substantial financial losses for users. Security threats on NFT Marketplaces include (but are not limited to):

- Wallet Vulnerabilities
- Marketplace vulnerabilities
- Smart contract vulnerabilities

With this in mind, NFT marketplaces should:

- strive to ensure their platforms are secure from threats of theft and other malicious online activities through regular security audits of their marketplace, smart contracts, and wallets (for those entities providing custodial services).
- comply with all applicable laws.
- ensure transaction records are maintained for the requisite periods and can be accessed when needed.
- ensure their service terms are kept up-to-date and regularly updated and communicated to users.
- comply on a best-effort basis with the Guidance for business-to-consumer electronic commerce transactions published by the International Standards Organisation under ISO 10008:2022.[24]

Effective **R**edressal of Complaints: NFT marketplaces should be responsive to consumer complaints and put mechanisms in place to address them in a timely manner. To that end, NFT marketplaces should:

- establish an adequate grievance redressal mechanism that provides users with a mechanism to report violations. having regard to the number of grievances ordinarily received by such entity from India, and should appoint a grievance officer for consumer grievance redressal. The marketplace should display the name, contact details, and designation of such officer on its platform.[25] Details about such grievance redressal mechanisms should be made clear and apparent and accessible to all users through the platform interface.
- respond in a timely manner to such consumer complaints. Timelines for response (and for measures such as disbursal of refunds, if applicable) should be made clear.

[24] Available at https://www.iso.org/obp/ui/#iso:std:iso:10008:ed-2:v1:en
[25] Rule 4(4) Consumer Protection (E-Commerce) Rules, 2020, https://consumeraffairs.nic.in/sites/default/files/E%20commerce%20rules.pdf

- clarify the extent of seller verification, and correspondingly the extent to which buyers can take action against sellers (For example: if platforms are permitting users to be pseudonymous by not disclosing personally identifiable information, they should give warnings about seller fraud and highlight to consumers that recourse might be limited on the page of the seller in question).
- comply on a best efforts basis with the Guidelines for complaints handling in organizations published by the International Standards Organisation under ISO 10002:2018.[26]

Checklist

Safety from Harm through **A**wareness: The NFT Marketplace has:

[26] Available at https://www.iso.org/obp/ui/#iso:std:iso:10002:ed-3:v1:en.

- Instituted a system of age-gating/parental consent at the time of sign-up
- Created a program for seller verification
- Clearly indicated the liability of sellers (verified and unverified) in their policies
- Included relevant information about sellers, including a rating system
- Provided for feedback from verified purchasers about seller quality, while complying on best effort basis to Bureau of Indian Standards' IS 19000:2022 on 'Online Consumer Reviews – Principles and Requirements for their Collection, Moderation and Publication'.
- Required sellers to provide undertakings about the veracity and accuracy of the products they are selling.
- Provided attribute indicators for each work sold, as described in the Standards
- Ensured all advertisements carry disclaimers about the risks of investing in digital assets.
- Not engaging in any unfair trade practices
- Made clear disclosures about conflicts of interest.
- Been transparent about pricing and fees, which includes adding details of NFT's purchase price and transaction history clearly in their User Interface.

Fortification: The NFT Marketplace has:

- Put in place policies for regular security audits of the site, smart contracts, and wallets (for those entities providing custodial services).
- Complied with the latest guidelines on cyber-security (from CERT-In) and followed international best practices.
- Ensured transaction records are accessible and maintained for the requisite periods
- Kept service terms up-to-date and regularly communicated to users.
- Complied on a best-effort basis with the Guidance for business-to-consumer electronic commerce transactions published by the International Standards Organisation under ISO 10008:2022.

Effective **R**edressal of Complaints: The NFT Marketplace has:

- Provide users with a clear mechanism to report violations.
- Established internal processes and timelines for addressing consumer complaints.
- Appointed a grievance officer for consumer grievance redressal, whose details are displayed prominently on the platform.
- Clearly and prominently displayed information required for compliance
- Clarified the extent of seller information they possess
- Complied on a best efforts basis with the Guidelines for complaints handling in organizations published by the International Standards Organisation under ISO 10002:2018.

The SAFER Standards for NFT Marketplaces are now up for consultation. Please share your comments on the standards by 1 September 2023 with consultations@emergingtechindia.com.