 ***DOI:** https://doi.org/10.63108/IJLMH.12816*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

When Does Cybercrime Become 'Organised Crime'? Interpreting the Threshold of 'Continuing Unlawful Activity' under Section 111 of the Bharatiya Nyaya Sanhita, 2023

DR. CUMARAN NADARADJAN*

ABSTRACT

Section 111 of the Bharatiya Nyaya Sanhita, 2023 (BNS) places organised crime within India's general penal law and expressly includes cyber-crimes among the forms of conduct capable of falling within that offence. The inclusion is consequential, but it can also mislead. A cyber offence does not become organised crime merely because it is technologically sophisticated, financially large, committed by several persons, or spread across multiple jurisdictions. Section 111 requires a more demanding combination: continuing unlawful activity, an organised crime syndicate, a legally relevant nexus between the accused and that syndicate, specified unlawful means, and a material-benefit objective. This paper examines that threshold through the text of Section 111, the jurisprudence developed under the Maharashtra Control of Organised Crime Act, 1999 and the earliest High Court decisions applying the BNS provision. It argues that Section 111 should be interpreted as an enterprise-oriented offence rather than an aggravated form of ordinary cybercrime. Particular attention is given to recurring phishing and investment-fraud networks, mule-account structures, ransomware groups, decentralised digital syndicates, and the evidentiary problem of attributing membership or knowing participation in online criminal networks. The paper proposes a seven-part judicial framework designed to preserve Section 111 for durable criminal enterprises while preventing its routine use in ordinary multi-accused cyber-fraud prosecutions. Such an approach gives effect to legislative purpose without sacrificing legality, proportionality and individualised criminal responsibility.

Keywords: *Bharatiya Nyaya Sanhita, Section 111, organised crime, cybercrime, continuing unlawful activity, organised crime syndicate, digital fraud*

I. INTRODUCTION

Cybercrime has altered not only the scale of offending but also the architecture of criminal participation. A fraudulent operation may involve a caller in one State, a bank account opened

* Author is an Independent Legal Researcher and Advocate, Bar Council of Delhi, India. ORCID: https://orcid.org/0009-0005-7135-6543

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

in another, credentials stolen from a victim in a third, a server located outside India, and proceeds moved through several intermediaries before being converted into virtual assets. Those actors may never meet. They may know one another only through aliases. Their roles can be specialised, temporary and geographically dispersed. Yet the operation may function with a degree of continuity that resembles a conventional criminal enterprise.

The Bharatiya Nyaya Sanhita, 2023 (BNS) responds to that transformation by bringing organised crime into the general penal code. Section 111 expressly identifies "cyber-crimes" among the activities that may constitute organised crime.[1] The statutory choice is important. The Indian Penal Code, 1860 did not contain a comparable national offence, and organised-crime prosecution had largely depended on special State legislation, most notably the Maharashtra Control of Organised Crime Act, 1999 (MCOCA).[2]

The new provision, however, creates an interpretive risk. In ordinary speech, many cyber offences are "organised": they are planned, coordinated and committed by more than one person. The legal concept in Section 111 is narrower. Parliament did not say that a cybercrime committed by a group is organised crime. It tied the offence to "continuing unlawful activity," participation as a member of or on behalf of an "organised crime syndicate," specified unlawful means, and the object of obtaining direct or indirect material benefit.[3] The Explanation then defines continuing unlawful activity by reference to serious cognizable offences, a syndicate nexus, more than one charge-sheet within the preceding ten years and cognizance by a competent court.[4]

The central question is therefore not whether a cyber offence was organised in the colloquial sense. It is when cybercrime crosses the statutory boundary into the qualitatively different form of criminality that Section 111 is designed to punish.

That question has immediate practical consequences. Cyber-fraud investigations increasingly reveal networks of callers, account suppliers, cash-out agents, SIM-card procurers, domain administrators and cryptocurrency intermediaries. If the existence of several roles were sufficient, Section 111 could become a routine add-on to cheating, impersonation and computer-related offences. Such a reading would make the elaborate statutory definitions largely redundant. Conversely, an interpretation that assumes a traditional hierarchy, territorial gang or

[1] The Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023), § 111(1).
[2] The Maharashtra Control of Organised Crime Act, Maharashtra Act No. 30 of 1999, §§ 2(1)(d)–(f), 3.
[3] The Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023), § 111(1).
[4] *Id.* § 111(1) Explanation (ii).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

permanent leadership structure could make Section 111 ineffective against decentralised digital enterprises.

The first reported High Court decisions under the provision demonstrate the tension. In *Vinay Baghla v. State of Rajasthan*, the Rajasthan High Court stressed that Section 111 is directed at structured criminal enterprises and warned against mechanically treating a serious financial or cyber-fraud case involving multiple persons as organised crime.[5] In *Sidhartha Chandran v. State of Kerala*, the Kerala High Court treated the antecedent charge-sheet requirement as a real statutory condition and held, at the prima facie stage, that the provision was not attracted where the petitioner had no qualifying charge-sheet in the preceding ten years.[6] These cases suggest that the early judicial project under Section 111 will be one of boundary drawing.

This paper argues for an enterprise-oriented interpretation. Section 111 should not operate as an aggravated cybercrime provision triggered by scale, sophistication or plurality alone. Its distinctive function is to punish durable criminal enterprise: repeated unlawful activity linked to a syndicate that has enough continuity and organisational identity to outlive the single transaction under prosecution. The paper first examines the statutory architecture and its relationship with MCOCA jurisprudence. It then considers the concept of continuing unlawful activity, the meaning of a digital syndicate, individual attribution in mule-account and platform-based networks, the overlap with existing cybercrime law, and the constitutional implications of overbroad invocation. It concludes by proposing a seven-part judicial framework for deciding when a cybercrime network becomes an organised crime syndicate within Section 111.

II. Section 111 as an Enterprise Offence

Section 111 is best understood through the relationship among three concepts: the present act of organised crime, the "organised crime syndicate," and "continuing unlawful activity." The first concept describes the punishable conduct; the second supplies the collective structure; the third supplies continuity.

The provision covers continuing unlawful activity including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offence, cyber-crimes, trafficking and other specified conduct. But the list of activities is only the starting point. The activity must be undertaken by a person or group acting in concert, singly or jointly, either as a member of an

[5] *Vinay Baghla v. State of Rajasthan*, S.B. Criminal Revision Petition No. 1721/2025, 2026:RJ-JD:21961, ¶¶ 7.5–8.1 (Raj. H.C. May 18, 2026).
[6] *Sidhartha Chandran v. State of Kerala*, Bail Appl. No. 4750/2026, 2026:KER:65581, ¶¶ 6–15 (Ker. H.C. Aug. 21, 2026).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

organised crime syndicate or on behalf of it, through violence, threat, intimidation, coercion or other unlawful means, for direct or indirect material benefit.[7]

The statutory definition of an organised crime syndicate is equally significant. It refers to a group of two or more persons who, acting singly or jointly as a syndicate or gang, indulge in continuing unlawful activity.[8] The group requirement is therefore modest in numerical terms—two persons may suffice—but the group must be linked to continuing unlawful activity. Mere plurality is not the same as syndicate identity.

The definition of continuing unlawful activity creates the principal gate. The activity must be prohibited by law, constitute a cognizable offence punishable with imprisonment of three years or more, be undertaken by a person singly or jointly as a member of or on behalf of an organised crime syndicate, and be one in respect of which more than one charge-sheet has been filed before a competent court during the preceding ten years and cognizance taken.[9] The statute thus refuses to define organised crime solely by the gravity of the present allegation. It demands a legally cognizable history of criminal activity linked to the enterprise.

This architecture strongly resembles MCOCA. Supreme Court jurisprudence under MCOCA has treated continuing unlawful activity, organised crime, and organised crime syndicate as closely interrelated statutory concepts. In *State of Maharashtra v. Bharat Shanti Lal Shah*, the Court upheld the core organised-crime framework while recognising the special character of the regime.[10] In *Zameer Ahmed Latifur Rehman Sheikh v. State of Maharashtra*, the Court again approached the statutory concepts as part of a single legislative scheme.[11] Later, in *State of Maharashtra v. Shiva @ Shivaji Ramaji Sonawane*, the Court made clear that historical charge-sheets do not by themselves constitute the new offence: there must be relevant organised criminal activity after the statute becomes operative.[12] The Supreme Court reaffirmed that proposition in *State of Gujarat v. Sandip Omprakash Gupta* while construing the analogous Gujarat statute.[13]

The continuity of language matters. Parliament legislated in 2023 against a body of organised-crime jurisprudence developed over more than two decades. The BNS is not identical to MCOCA, and precedent cannot simply be transplanted without attention to wording and

[7] The Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023), § 111(1).
[8] *Id.* § 111(1) Explanation (i).
[9] *Id.* § 111(1) Explanation (ii).
[10] *State of Maharashtra v. Bharat Shanti Lal Shah*, (2008) 13 SCC 5 (India).
[11] *Zameer Ahmed Latifur Rehman Sheikh v. State of Maharashtra*, (2010) 5 SCC 246 (India).
[12] *State of Maharashtra v. Shiva @ Shivaji Ramaji Sonawane*, (2015) 14 SCC 272 (India).
[13] *State of Gujarat v. Sandip Omprakash Gupta*, Criminal Appeal No. 2291 of 2022, 2022 INSC 1288 (S.C. Dec. 15, 2022) (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

context. Nevertheless, where Parliament adopts established legal terms of art—particularly "continuing unlawful activity" and "organised crime syndicate"—earlier judicial treatment provides a valuable interpretive starting point.

The enterprise-oriented reading also explains why Section 111 sits awkwardly if treated as an ordinary offence enhancement. Cheating, identity fraud, forgery, conspiracy and computer-related offences already punish discrete wrongdoing. Section 111 is justified only if it captures an additional social harm: the institutionalisation of criminal activity through a durable network capable of repeating offences, replacing participants, reusing infrastructure and extracting material benefit over time. That danger is different in kind from the danger posed by a single, even very serious, cyber fraud.

III. "CYBER-CRIMES" DOES NOT CREATE A SHORTCUT

The express reference to cyber-crimes in Section 111 is both useful and potentially misleading. It confirms that an organised criminal enterprise may be digital, borderless and technologically mediated. It does not create a presumption that cybercrime is organised crime.

Cyber offences frequently exhibit features that resemble organisation. A phishing operation may involve script writers, callers, account suppliers and cash-out agents. A fraudulent investment platform may employ a website administrator, social-media promoters and persons controlling settlement accounts. Ransomware operations may divide functions among developers, access brokers, affiliates and money launderers. Even relatively small scams can involve several participants and substantial planning.

But ordinary criminal law already knows how to deal with concerted conduct. Conspiracy is not organised crime merely because several actors share a criminal design. Common intention does not become syndicate membership merely because the group uses digital tools. Abetment does not turn into continuing unlawful activity merely because assistance is repeated over a short period.

The key distinction is between a transaction and an enterprise. A transaction may be elaborate, profitable and multi-person. An enterprise has an organisational identity and temporal life that are not exhausted by the particular offence before the court.

Consider a one-time online investment fraud. Four people create a false platform, run an aggressive advertising campaign for three weeks and obtain several crores from victims before shutting down. The facts may support numerous serious offences. Yet without the antecedent and syndicate requirements, the monetary scale and victim count cannot independently satisfy

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Section 111. The enterprise inquiry asks whether there is continuing unlawful activity of the statutory kind and whether the accused acted as a member of, or on behalf of, a qualifying syndicate.

Now consider a recurring phishing operation that has existed for several years. It rotates domains and phone numbers, recruits callers, maintains common scripts, repeatedly uses the same laundering channels, and replaces compromised accounts and devices. Members have qualifying prior charge-sheets and the group persists despite arrests. This is much closer to the institutionalised criminality at which Section 111 is directed.

The difference is not "online versus offline" or "small versus large." It is the existence of continuity, syndicate identity and purposeful participation. The statutory phrase "cyber-crimes" identifies a field of predicate conduct; it cannot do the work of the remaining elements.

That approach is consistent with *Vinay Baghla*. The Rajasthan High Court described Section 111 as an architecturally distinct provision aimed at structured criminal enterprises and cautioned that the mere presence of multiple offenders or serious allegations cannot replace the foundational material required by the statute.[14] The judgment is especially important because the temptation to over-classify is strongest in financial cybercrime, where complex transaction chains can create an appearance of a single syndicate even when the evidence shows only temporary or indirect connections.

IV. Continuing unlawful activity as a gatekeeper

The phrase "continuing unlawful activity" should be treated as the main statutory gatekeeper. Each component performs a distinct limiting function.

First, the underlying activity must be prohibited by law and constitute a cognizable offence punishable with imprisonment of three years or more. Section 111 is therefore not designed to convert regulatory non-compliance or minor digital wrongdoing into organised crime. The gravity threshold is express.

Second, the activity must be undertaken as a member of an organised crime syndicate or on its behalf. This requirement is relational. A criminal record does not establish organised crime merely because it demonstrates repetition. The antecedent activity must have the legally relevant syndicate connection.

Third, the statute requires more than one charge-sheet within the preceding ten years and cognizance by the competent court. "More than one" ordinarily means at least two. The

[14] *Vinay Baghla*, 2026:RJ-JD:21961, ¶¶ 7.5–8.1.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

cognizance requirement is important because it prevents raw police allegations alone from constituting the statutory history. Although cognizance is not a finding of guilt, it inserts a judicial act into the antecedent chain.

The Kerala High Court's decision in *Sidhartha Chandran* illustrates the point. The petitioner's bank account was alleged to have been used to facilitate cybercrime. The prosecution nevertheless conceded that there was no qualifying charge-sheet against him within the statutory period. The Court held, on a prima facie assessment, that Section 111 could not be sustained in the absence of that condition.[15] The decision is particularly relevant to cybercrime because the investigative visibility of a bank account can tempt authorities to infer syndicate membership from transaction flow alone.

There is, however, a further interpretive question: whose antecedents matter? MCOCA jurisprudence has often distinguished between the antecedent activity of the syndicate and the personal antecedents of the individual accused. Section 111's text must be read carefully before assuming that every accused must personally be named in every qualifying prior charge-sheet. At the same time, the provision cannot be reduced to a theory under which a person with no meaningful connection to earlier syndicate activity becomes liable for organised crime merely because the prosecution can point to prior cases involving someone in the alleged network.

The better approach is to keep two inquiries separate. The first is enterprise continuity: does the alleged syndicate satisfy the statutory history of continuing unlawful activity? The second is individual nexus: is there evidence that the present accused acted as a member of or on behalf of that continuing enterprise with the mental element required for the particular form of liability alleged? This avoids confusing the history of the organisation with the culpability of an individual.

The antecedent requirement should also not be treated as sufficient. Two prior charge-sheets and cognizance do not automatically establish organised crime in the present case. Shiva and *Sandip Omprakash Gupta* are instructive on this point. Those decisions emphasise that the present prosecution must involve conduct amounting to the substantive organised-crime offence; old cases cannot themselves be repackaged as the new offence.[16] The same logic should govern Section 111. Historical continuity is necessary to the statutory architecture, but current organised criminal conduct must still be proved.

[15] *Sidhartha Chandran*, 2026:KER:65581, ¶¶ 5, 15.
[16] *Shiva @ Shivaji Ramaji Sonawane*, (2015) 14 SCC 272; *Sandip Omprakash Gupta*, 2022 INSC 1288.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

V. What is a digital "organised crime syndicate"?

The term "syndicate" cannot be frozen in an image of twentieth-century organised crime. Digital criminal enterprises may be decentralised, fluid and pseudonymous. Members may never meet in person. Functions may be outsourced. Infrastructure may be rented. A network may have no permanent headquarters and no single leader. Yet it may still possess continuity, role differentiation, profit-sharing and a stable operational identity.

Courts should therefore avoid two opposite errors. The first is excessive rigidity: requiring a mafia-style hierarchy, territorial control or formal membership before recognising a cyber syndicate. That would make Section 111 easy to evade through decentralised design. The second is excessive elasticity: calling any connected group of digital actors a syndicate. That would collapse the concept into ordinary conspiracy.

A useful question is whether the alleged group has an existence and capacity for criminal action beyond the incident charged. Several indicators may be relevant: persistent role allocation; repeated use of shared infrastructure; common financial channels; recurring victim-selection methods; recruitment and replacement mechanisms; revenue-sharing arrangements; common command or coordination processes; reuse of accounts, domains, devices or wallets; and continuity despite changes in individual membership.

None of these indicators is independently decisive. A shared IP address can reflect common infrastructure without common criminal intent. A cryptocurrency transfer can show financial connection without proving syndicate membership. Presence in a Telegram or WhatsApp group may show association rather than agreement. The legal conclusion must arise from the totality of proven relationships, not from technological labels.

The distinction between a "network" and a "syndicate" is especially important. A network describes connection. A syndicate, in the statutory sense, describes organised criminal enterprise. Many people may use the same laundering service or illicit online marketplace without forming one organised crime syndicate. Likewise, independent fraudsters may purchase access credentials from the same broker without sharing enterprise identity.

Prosecutors should therefore be required to identify the particular syndicate alleged with reasonable specificity. Who forms the group? What functions link its members? What shows that its operations persist beyond one transaction? What prior activity supplies the statutory continuity? What is the accused's relationship to the group? Without answers to these questions, the term "cyber gang" risks becoming rhetoric rather than legal proof.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

VI. MULE ACCOUNTS, INTERMEDIARIES AND INDIVIDUAL ATTRIBUTION

Mule-account cases expose the danger of guilt by association more clearly than almost any other form of cybercrime prosecution. Fraud proceeds often move through chains of bank accounts before withdrawal or conversion. The account holder is visible to investigators; the true controller may be remote or unknown. The evidentiary convenience of account ownership can therefore produce an inference stronger than the underlying facts justify.

Not every account holder occupies the same position. One person may knowingly sell control of an account for commission. Another may repeatedly receive and forward funds with full awareness of the fraud network. A third may be reckless about how the account is used. A fourth may have been deceived into providing credentials. A fifth may be a victim of identity misuse. Section 111 cannot erase these distinctions.

Where membership, facilitation, abetment or proceeds-based liability is alleged, courts should insist on evidence of the particular mental and organisational nexus. Relevant facts may include repeated use of the account, receipt of commission, communications with network organisers, deliberate transfer of credentials, coordinated withdrawals, use of multiple accounts, efforts to conceal the transaction trail, and continued participation after suspicious activity became obvious. The inference becomes stronger where the same person performs a defined function for repeated offences or has links to the enterprise's common infrastructure.

The reverse proposition is equally important: transaction proximity is not membership. A person does not become part of an organised crime syndicate merely because money from a criminal enterprise passed through an account bearing that person's name. Nor does a service provider automatically become a syndicate member because criminals used the service.

The general presumption that mens rea remains significant in penal liability reinforces this approach. In the MCOCA context, Bharat Shanti Lal Shah recognised the need to construe extraordinary penal provisions within constitutional limits.[17] Section 111 extends liability to abetment, conspiracy, facilitation, preparatory conduct, membership, harbouring and possession of proceeds in different ways. Those extensions make individualised analysis more, not less, important.

Cybercrime produces difficult attribution problems. But difficulty of proof cannot justify dilution of the elements. The State may use digital forensics, transaction analysis, device

[17] *Bharat Shanti Lal Shah*, (2008) 13 SCC 5.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

evidence and communications to establish knowing participation. What it cannot do is substitute connectivity for culpability.

VII. Ransomware, phishing and decentralised criminal enterprises

Different cybercrime models illustrate why Section 111 requires a functional rather than formal approach to organisation.

A recurring phishing network may be comparatively centralised. It can have managers, callers, script writers and withdrawal teams. Its continuity may be demonstrated by repeated campaigns, common technical infrastructure, recurring laundering channels and replacement of compromised personnel. If the statutory antecedents are present, such a model can fit Section 111 without conceptual difficulty.

Ransomware-as-a-service presents a more complex structure. Developers may maintain malware and payment infrastructure while affiliates select targets and conduct intrusions. Access brokers may supply compromised credentials, and specialist services may launder cryptocurrency. Participants need not know every member. The enterprise can nevertheless be stable because the platform, revenue-sharing model and criminal service persist across attacks. The absence of a conventional hierarchy should not defeat organised-crime liability where the prosecution proves the required syndicate and continuity.

By contrast, a one-time collaboration formed around a single target should not be converted into a syndicate merely because participants divided tasks. The defining question is whether the group's criminal identity and operational capacity persist independently of the particular offence.

This distinction also matters for rapidly assembled online groups. Digital platforms make it easy to recruit temporary participants for a single operation. A person can rent infrastructure, purchase stolen data and engage an anonymous cash-out service without creating a continuing enterprise among all participants. Courts should resist the assumption that a supply chain is necessarily a syndicate. The prosecution must show a legally coherent group, not merely a sequence of transactions among offenders.

The same principle applies to "crime-as-a-service" ecosystems. A marketplace can facilitate repeated crime by many independent users. It may itself constitute an organised enterprise if its operators meet the statutory conditions. But customers of the marketplace do not automatically become members of the same syndicate. Organised-crime attribution must remain group-specific and accused-specific.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

VIII. Section 111 within India's fragmented cybercrime framework

Section 111 does not operate in a vacuum. India's cybercrime law is distributed across the BNS, the Information Technology Act, 2000 and sector-specific legislation. Computer-related offences may be prosecuted under the Information Technology Act, while cheating, personation, forgery, criminal breach of trust, conspiracy and proceeds-related conduct may attract provisions of the general penal law.[18]

The organised-crime provision should therefore have a distinctive doctrinal role. The underlying offence identifies the prohibited act. Conspiracy and abetment allocate responsibility for collaboration. Section 111 should address the additional enterprise dimension: continuing unlawful activity conducted through a qualifying syndicate for material benefit.

If Section 111 is treated merely as a more serious version of cyber fraud, duplication becomes endemic. Every large phishing case could be charged simultaneously as cheating, conspiracy, computer-related crime and organised crime without a principled explanation of what the last charge adds. That would weaken rather than strengthen the coherence of the criminal law.

The overlap is even more complicated in States with special organised-crime statutes. The BNS creates a national offence while MCOCA and analogous State laws remain on the books. Legislative analysis during the enactment of the new criminal codes noted the possibility of duplication between the BNS organised-crime provision and State organised-crime regimes.[19] Prosecutorial choice may therefore determine not only the label of the offence but also the procedural environment in which an accused is investigated and tried.

A national charging policy would be useful. It should explain when Section 111 is preferred over an applicable special State statute, how duplicate charges are to be handled, and what approval is required before the organised-crime provision is added to a cybercrime case. Such guidance would reduce arbitrary variation across jurisdictions while preserving prosecutorial flexibility for genuinely complex enterprises.

IX. Constitutional and rule-of-law limits

The breadth and severity of organised-crime liability make interpretive discipline a constitutional concern, not merely a drafting preference.

---

[18] The Information Technology Act, No. 21 of 2000, India Code (2000), §§ 43, 66, 66C, 66D; The Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).

[19] PRS Legislative Research, *Legislative Brief: The Bharatiya Nyaya Sanhita, 2023* (2023), https://prsindia.org/files/bills_acts/bills_parliament/2023/Legislistive_Brief-Bharatiya_Nyaya_Sanhita_2023.pdf (discussing the overlap between the proposed organised-crime offence and State organised-crime laws).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Article 14 requires non-arbitrary application of criminal law. If similar cyber-fraud conduct is treated as ordinary cheating in one case and as organised crime in another solely because investigators use different labels, the distinction becomes vulnerable to arbitrariness. A structured threshold encourages like cases to be treated alike.

Article 21 is equally relevant. Section 111 carries severe punishment and substantial stigma. The liberty consequences of invoking the provision are therefore greater than those associated with many ordinary predicate offences. Judicial scrutiny at bail, cognizance and charge-framing stages should reflect that reality while respecting the limited nature of each procedural inquiry.

Proportionality provides a further reason for preserving the enterprise threshold. Organised crime warrants exceptional punishment because a durable criminal organisation can repeatedly generate harm, mobilise resources, replace participants and survive individual prosecutions. If the prosecution cannot show those characteristics, much of the normative basis for treating the conduct as organised crime disappears.

The Supreme Court's organised-crime cases demonstrate a broader principle: special or extraordinary criminal regimes must be applied according to the elements the legislature actually enacted. *Sandip Omprakash Gupta* refused to permit historical cases alone to create organised-crime liability where the statute required relevant post-commencement activity.[20] The point is not leniency. It is legality. Serious criminality does not authorise courts or prosecutors to omit statutory conditions.

Vinay Baghla brings that principle into Section 111. The Rajasthan High Court's insistence on objective foundational material for the syndicate, continuing unlawful activity and the accused's nexus is therefore not an obstacle to effective prosecution. It is a way of preserving the exceptional offence for the cases that justify it.

X. A SEVEN-PART JUDICIAL TEST FOR ORGANISED CYBERCRIME

The emerging jurisprudence would benefit from a structured method of analysis. The following seven-part framework is proposed as a way to organise the statutory inquiry. It is not a balancing test. The factors correspond to cumulative legal requirements; strength on one cannot cure the absence of another element that the statute makes mandatory.

[20] *Sandip Omprakash Gupta*, 2022 INSC 1288.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

A. Qualifying predicate conduct

The prosecution should identify the underlying activity prohibited by law and demonstrate that it satisfies the statutory seriousness threshold. The label "cybercrime" is not itself an offence and should never substitute for identification of the legal wrong alleged.

B. Statutory continuity

The prosecution should place material showing the qualifying history required by the definition of continuing unlawful activity: the relevant charge-sheets, the ten-year period and the orders showing cognizance. Where the continuity is said to attach to the syndicate rather than personally to every accused, the prosecution should explain the legal and evidentiary basis for that position.

C. Syndicate existence

There must be evidence of a group possessing sufficient organisational coherence to be described as a syndicate or gang. Two persons may satisfy the numerical minimum, but numerical plurality does not itself prove syndicate identity. Courts should look for recurring coordination, operational roles, shared infrastructure or other evidence showing a criminal organisation rather than an ad hoc collaboration.

D. Enterprise continuity

The organisation should have a temporal life extending beyond the single incident charged. Recurrent operations, re-used infrastructure, replacement mechanisms, continuing revenue arrangements, persistent victim-selection methods and recurring financial channels can all be relevant. This inquiry captures the difference between a transaction and an enterprise.

E. Accused–syndicate nexus

The prosecution must identify how the accused acted as a member of, or on behalf of, the syndicate. Communication, financial contact or presence in a digital group may be evidentiary pieces, but they should not be treated as conclusions. The court should look for purposeful participation, knowledge of the enterprise, defined function, repeated assistance or other facts supporting the required nexus.

F. Unlawful means and material-benefit objective

Section 111 expressly refers to violence, threat, intimidation, coercion or other unlawful means and to direct or indirect material benefit, including financial benefit.[21] In cybercrime cases,

[21] The Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023), § 111(1).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

"other unlawful means" will often carry much of the analytical burden. Courts should nevertheless require the prosecution to identify the unlawful method and benefit sought rather than assuming them from the predicate offence.

G. Present organised-crime conduct

Finally, the current prosecution must itself involve organised-crime conduct. Antecedent charge-sheets establish part of the statutory history; they do not prove the present offence. This principle follows the logic of Shiva and *Sandip Omprakash Gupta* and prevents criminal history from becoming a substitute for proof.[22]

The value of this framework is practical. It gives investigators a checklist for evidence collection, prosecutors a disciplined charging structure, and courts a transparent way to explain why Section 111 does or does not apply.

XI. Applying the Test to Common Cybercrime Scenarios

The proposed framework can be tested against recurring fact patterns.

A. One-time investment platform

Suppose four persons create a fraudulent investment website, advertise it through social media, receive money from hundreds of victims and close the operation after one month. The case is serious and coordinated. Yet the victim count and loss amount do not answer the Section 111 inquiry. If there is no qualifying continuing unlawful activity and no enterprise continuity beyond the single scheme, organised-crime liability should not arise merely because the fraud was large.

B. Recurring phishing syndicate

A group operates for years, rotates domains and SIM cards, recruits callers, uses common scripts, controls recurring mule-account channels and continues after individual arrests. Qualifying prior charge-sheets exist and cognizance has been taken. This is a much stronger Section 111 case because the enterprise persists beyond particular offences.

C. Ransomware service

A ransomware platform maintains malware, affiliate rules, payment infrastructure and a revenue-sharing model across repeated attacks. Membership changes but the platform remains. If Indian jurisdiction exists and the statutory antecedents and benefit requirements are proved, decentralisation should not prevent classification as a syndicate.

[22] *Shiva @ Shivaji Ramaji Sonawane*, (2015) 14 SCC 272; *Sandip Omprakash Gupta*, 2022 INSC 1288.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

D. Mule-account holder

A person opens one account and permits another to use it for a payment. Without evidence of knowing, purposeful and sufficiently connected participation, Section 111 membership should not follow. The prosecution may have other offences available, but organised crime requires proof of the additional enterprise nexus.

E. Repeat solo hacker

An individual repeatedly commits serious cyber offences alone. Repetition may demonstrate dangerous recidivism but does not automatically create an organised crime syndicate, whose definition requires a group of two or more persons.[23] The statute should not be rewritten merely because repeated solo offending appears organised in an everyday sense.

F. Shared criminal marketplace

Several independent fraudsters buy stolen credentials from the same online marketplace. The marketplace operators may constitute an organised syndicate if the statutory conditions are met. The buyers, however, do not automatically belong to that same syndicate. The prosecution must identify the particular criminal enterprise and the accused's relationship to it.

These examples show why Section 111 should be applied by legal structure rather than intuition. Technological complexity can make conduct look more integrated than it is. The law must distinguish transactional connection from enterprise membership.

XII. Investigation and Prosecution: What Should Be Proved

A disciplined threshold does not make organised cybercrime impossible to prosecute. It changes the evidentiary focus from the isolated transaction to the enterprise.

Investigators should map relationships across time. Useful material may include repeated communication patterns; common device or account control; recurring domains and servers; wallet relationships; recruitment communications; revenue-sharing arrangements; instructions allocating roles; repeated victim-selection methods; replacement of compromised accounts; and documentary proof of qualifying prior prosecutions.

Digital evidence is particularly well suited to demonstrating relational patterns, but its interpretation must be cautious. A common IP address may indicate shared infrastructure or a commercial service. A wallet transfer may establish a payment but not the purpose or mental state behind it. A messaging-group membership may establish access rather than agreement.

[23] The Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023), § 111(1) Explanation (i).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The evidentiary task is to combine multiple facts into a legally coherent account of enterprise and individual role.

Prosecutors should also be required, as a matter of policy, to prepare a written Section 111 statement before filing or sustaining the organised-crime charge. That statement should identify the alleged syndicate; the qualifying continuing unlawful activity; the relevant prior charge-sheets and cognizance orders; the present organised-crime act; the accused's role; the unlawful means; and the material benefit sought. A requirement of this kind would not create a new element of the offence. It would simply force the prosecution to articulate how the existing elements are said to be met.

Such discipline would also improve judicial review at the charge stage. A court need not conduct a mini-trial. But where the prosecution material, taken at the applicable threshold, is incapable of showing an essential statutory ingredient, the extraordinary charge should not survive merely because ordinary offences are plainly disclosed.

That distinction is important. Removing Section 111 from a case does not immunise fraud, conspiracy, identity theft or other cybercrime. It ensures only that the legal label corresponds to the conduct proved.

XIII. Reform and clarification

Several aspects of Section 111 would benefit from authoritative clarification as case law develops.

First, courts should clarify the relationship between the syndicate's antecedent activity and the individual accused's personal criminal history. The statutory text should not be applied in a manner that makes prior charge-sheets against every present accused invariably necessary if the enterprise itself satisfies the continuity requirement; nor should the history of remote actors be enough to draw a newcomer into organised-crime liability without proof of knowing participation. The two inquiries—enterprise continuity and individual nexus—should remain analytically separate.

Second, the interaction between Section 111 and State organised-crime statutes requires policy guidance. Where overlapping regimes are available, prosecutors should explain the basis for selecting one framework over another, especially if procedural consequences differ materially.

Third, law-enforcement training should emphasise that "cyber gang," "mule account" and "syndicate transaction" are investigative descriptions, not substitutes for legal elements. The

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

proper sequence is facts, statutory ingredients, then legal conclusion—not label, assumption, then liability.

Fourth, cybercrime-specific investigation manuals should focus on evidence of continuity and organisational identity: role persistence, reuse of infrastructure, recruitment practices, financial distribution and historical operations. That evidence is more probative of enterprise than the mere number of accounts or transactions.

Fifth, courts should continue to insist on proportionality at the level of statutory interpretation. Section 111 is most legitimate when its extraordinary consequences are reserved for the extraordinary criminal structure the legislature defined.

A further uncertainty concerns the temporal relationship between antecedent activity and the present offence. The ten-year look-back period should not be treated as a licence to assemble unrelated prosecutions merely because they fall within the calendar window. The charge-sheets relied upon should be capable of supporting the proposition that the alleged syndicate engaged in continuing unlawful activity, not simply that one or more accused persons have accumulated a criminal record. Otherwise, the statutory term "continuing" loses its organisational meaning and becomes a synonym for recidivism. The distinction matters because a repeat offender may be dangerous without belonging to a durable criminal enterprise.

The same concern arises when the membership of a digital group changes over time. Cybercrime enterprises frequently replace callers, account suppliers or technical operators. A rule requiring identical membership across all predicate cases would be unrealistically rigid. But the opposite rule—allowing any historical charge-sheet against any person remotely connected to the present network—would be dangerously loose. Courts should look for continuity of enterprise identity: recurring command structures, operational methods, shared infrastructure, common revenue channels or other features demonstrating that the earlier and present conduct belong to the same criminal undertaking.

A related issue is the effect of acquittal, discharge or quashing in antecedent cases. Section 111 speaks of charge-sheets and cognizance rather than convictions, which shows that Parliament did not make prior conviction a textual precondition. Yet later judicial termination of an antecedent case may affect the weight or legal availability of that case as a foundation for continuing unlawful activity. This question will require careful appellate treatment. At minimum, prosecutors should disclose the current procedural status of every antecedent matter relied upon, and courts should not permit a stale or legally extinguished proceeding to be invoked without analysis.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

There is also a need to separate statutory interpretation from investigative convenience. Cybercrime investigations often begin with data clusters—accounts, devices, IP addresses and telephone numbers. These clusters are useful for identifying relationships, but Section 111 ultimately requires a legal theory of enterprise. Investigators should therefore build a chronology of the alleged syndicate: when it began, which activities demonstrate continuity, how roles were allocated, how proceeds were distributed, and what evidence connects the present accused to that history. A chronology of this kind would make the organised-crime allegation testable rather than impressionistic.

Finally, appellate courts should develop clear standards for the procedural stage at which each element must be demonstrated. The evidentiary burden at bail is not the burden at trial, and charge-framing does not require proof beyond reasonable doubt. But a lower procedural threshold is not the same as no threshold. Where the prosecution record contains no material capable of showing a qualifying antecedent, syndicate identity or accused–syndicate nexus, the seriousness of the underlying cyber fraud should not be allowed to fill the gap. The discipline of identifying what must ultimately be proved is essential even at preliminary stages.

XIV. Conclusion

Section 111 of the Bharatiya Nyaya Sanhita represents a major change in Indian criminal law. It gives prosecutors across the country a general penal provision directed at organised crime and expressly recognises that modern criminal enterprises can operate through cybercrime. That recognition is both necessary and overdue. Digital fraud networks, ransomware operations and transnational laundering structures can exhibit precisely the continuity, specialisation and replacement capacity associated with organised criminal enterprise.

The difficulty lies in preserving the boundary Parliament wrote into the law.

Cybercrime does not become organised crime merely because it is committed online, causes enormous financial loss, uses sophisticated technology, involves several accused or crosses State borders. Nor does repeat offending by itself establish a syndicate. Section 111 requires continuing unlawful activity of the statutory kind, an organised crime syndicate, a legally sufficient accused–syndicate nexus, qualifying unlawful means, a material-benefit objective and a present act amounting to organised crime.

The early High Court decisions are significant because they resist the easiest route to over-expansion. *Vinay Baghla* treats organised crime as a distinct form of enterprise criminality rather than an aggravated label for serious fraud. *Sidhartha Chandran* demonstrates that the antecedent charge-sheet requirement is not decorative statutory language. Together with the Supreme

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Court's jurisprudence under MCOCA and the Gujarat Control of Terrorism and Organised Crime Act, 2015, these decisions support an interpretation in which continuity is real, syndicate identity is proved, and individual culpability remains central.

The seven-part framework proposed in this paper—qualifying predicate conduct, statutory continuity, syndicate existence, enterprise continuity, accused–syndicate nexus, unlawful means and material benefit, and present organised-crime conduct—offers a practical method for applying those principles to digital cases. It also captures the essential proposition of this article: organised cybercrime is defined not by the presence of technology, but by the presence of a continuing criminal enterprise.

That distinction should guide the future development of Section 111. A narrow but workable threshold does not weaken the law. It protects its legitimacy, improves charging discipline and preserves severe organised-crime liability for the networks that truly possess the persistence and structure Parliament intended to confront.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]