

Forum Posts and Predicate Acts: Testing the Racketeering Statute Against Online Criminal Networks

Mohan Sanjay Wakhare¹, Dr. Shivanjali Bhoite²

^{1,2}*P.E. S Modern Law College and Ph.D. Research Centre Pune*

Abstract—The Racketeer Influenced and Corrupt Organizations Act was drafted in 1970 with the American mafia in view, yet prosecutors now invoke it against groups that look nothing like a crime family: dispersed, pseudonymous, and held together by a web forum rather than a boss and a neighbourhood. This paper asks whether the statute can carry that weight. It argues that the enterprise element, often assumed to be the obstacle, is in fact the easiest to satisfy, because an association-in-fact needs no hierarchy and online networks readily show shared purpose, working relationships, and longevity. The genuine pressure points lie elsewhere: a closed list of predicate offences that omits the principal computer-intrusion statute; continuity doctrine strained by crews that rebrand every few months; the separate inquiries into domestic conduct and domestic injury; proximate-cause limits on civil plaintiffs; and forfeiture rules written for physical assets. Drawing on the Infraud Organization prosecution, the Supreme Court’s racketeering decisions, and comparative treaty and statutory models, the paper concludes that RICO remains a workable instrument against cybercriminal networks, provided Congress closes the predicate gap, prosecutors keep exercising restraint, and courts hold the domestic-conduct inquiry to a disciplined standard.

Index Terms—Racketeering; Cybercrime; Association-In-Fact Enterprise; Extraterritoriality; Organised Crime

I. INTRODUCTION

In February 2018, federal prosecutors in Nevada unsealed an indictment against thirty-six people said to run the Infraud Organization, an online marketplace for stolen payment-card data whose motto was “In Fraud We Trust.”¹ The defendants came from the United States, Ukraine, Pakistan, Egypt, Russia, and several other countries, and arrests were made in seven. The government put actual losses above \$530 million.² The charging instrument was a racketeering conspiracy. Nothing about the group resembled the social clubs and union locals that Congress passed ‘the Racketeer Influenced and Corrupt Organizations Act (RICO)’ forty-eight years earlier.³

That mismatch is the starting point for this paper. The law reaches well beyond organised crime in the colloquial sense, and that its breadth is a product of its drafting rather than a mistake.⁴ Still, there is a difference between a statute that has been stretched to cover securities fraud and commercial disputes and one that must now cover a criminal economy conducted through encrypted channels, rented infrastructure, and cryptocurrency. The reported scale of that economy is considerable. The FBI’s Internet Crime Complaint Center received more than a million

¹ Press Release, U.S. Dep’t of Just., Thirty-Six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More Than \$530 Million in Losses from Cybercrimes (Feb. 7, 2018), <https://www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-criminal-organization-responsible> [hereinafter Infraud Press Release]. The indictment’s allegations are untested accusations, and the defendants are presumed innocent.

² *Id.* The release reports actual losses above \$530 million and intended losses of roughly \$2.2 billion.

³ Organized Crime Control Act of 1970, Pub. L. No. 91-452, tit. IX, 84 Stat. 922, 941 (codified as amended at 18 U.S.C. §§ 1961–1968).

⁴ See *H.J. Inc. v. Nw. Bell Tel. Co.*, 492 U.S. 229, 248–49 (1989) (explaining that RICO’s application to situations Congress did not expressly anticipate shows the statute’s breadth, not any ambiguity); *Sedima, S.P.R.L. v. Imrex Co.*, 473 U.S. 479, 499 (1985).

complaints in 2025 and recorded nearly \$21 billion in reported losses.⁵

The question here is narrow. Does RICO's text, as the courts have construed it, fit online criminal networks well enough to be worth using, and if not, where exactly does it fail? The answer offered below is that the usual worry is misplaced. Courts have long since freed the "enterprise" requirement from any need for hierarchy, and a forum or a botnet-for-hire crew fit comfortably within it. The strain appears in four other places: the list of predicate offences, the continuity requirement, the geographic limits on the statute's reach, and the remedies. Each is taken in turn, followed by a short comparison with the treaty definitions and an Indian statutory model that handle the same problem differently, and by a proposal for a limited amendment.

II. THE STATUTORY FRAME

RICO provides that it is illegal to use the profits derived from racketeering to fund an enterprise; to obtain or retain an ownership position in an enterprise via racketeering;⁶ to operate the business of an enterprise using a pattern of racketeering activities;⁷ or to enter into a conspiracy to engage in such conduct. There are two structures within the law. An "enterprise" can include both entities formed under law and unions and other groups of people who associate together but have no formal legal status.⁸ To establish a "pattern of racketeering activity," there must be at least two instances of racketeering within a ten-year period.⁹ In addition, "racketeering activity" is defined by a finite list of state and federal crimes, which Congress periodically updates. Penalties under RICO can be very harsh. The convicted can receive up to 20 years in prison. If the underlying crime is punishable by life imprisonment, then the sentence

will be life. Individuals found guilty can lose all of the money they obtained through their illegal activities as well as any interests they have in the enterprise.¹⁰ Private plaintiffs who suffer losses to their businesses or properties as a result of violations of RICO can seek triple damages.¹¹

Two features of the law's design matter for what follows. First, the statute separates the group from the conduct. The enterprise is one element and the pattern is another, and the government must prove both; the Supreme Court has said as much, describing the enterprise as organization.¹² Second, Congress told courts to read the Act liberally to achieve its remedial purposes.¹³ These choices explain why the statute has proved adaptable, and why its weak points lie in the lists and thresholds Congress drew rather than in the conceptual core.

III. THE ENTERPRISE PROBLEM THAT IS NOT A PROBLEM

A common intuition holds that a racketeering statute presupposes a stable criminal organisation with ranks, rules, and territory. Early commentary on RICO emphasised its capacity to reach people through their association with criminal groups rather than through any single act.¹⁴ Carried over to the internet, that picture suggests trouble, since carding forums, ransomware affiliate programs, and botnet rental markets are loose, fluid, and often anonymous.

The Supreme Court closed off that line of argument in *Boyle v. United States*.¹⁵ The case itself involved a loosely organised crew that stole from bank night-deposit boxes across several states, recruiting helpers as needed and, as the Court noted, apparently without a leader or hierarchy.¹⁶ If that crew qualified, a forum with an administrator, moderators, vendors, and thousands of registered users has little difficulty.

⁵ Fed. Bureau of Investigation, Internet Crime Complaint Ctr., 2025 Internet Crime Report (2026). The report was released on April 7, 2026.

⁶ 18 U.S.C. § 1962(a)–(d).

⁷ *Id.* § 1961(4).

⁸ *Id.* § 1961(5).

⁹ *Id.* § 1961(1).

¹⁰ *Id.* § 1963(a).

¹¹ *Id.* § 1964(c).

¹² *United States v. Turkette*, 452 U.S. 576, 583 (1981).

¹³ Organized Crime Control Act of 1970 § 904(a), 84 Stat. at 947.

¹⁴ *See, e.g.*, Gerard E. Lynch, *RICO: The Crime of Being a Criminal, Parts I & II*, 87 Colum. L. Rev. 661 (1987).

¹⁵ *Boyle v. United States*, 556 U.S. 938, 946 (2009).

¹⁶ *Id.* at 948.

Infraud illustrates the point. According to the indictment's summary, the group was created in October 2010, operated a forum that listed more than ten thousand registered members by March 2017, ran an escrow service for digital-currency payments, and was organized into administrators who approved membership and super-moderators who policed subject areas.¹⁷ A court asked whether those facts show purpose, relationships, and longevity would struggle to say no. The harder cases are the leaderless ones. Intrusion specialists who sell access to one another through a private channel, with no common brand and no relationship beyond individual transactions, could fall short of the second and third Boyle features, and the government would need evidence of coordination rather than arm's-length sales. That is a question of proof, not doctrine. Scholars were pointing out in the early 2000s that online criminal collaboration tends toward fluid, networked arrangements rather than the fixed hierarchies of traditional organized crime, and the law of enterprise had, by then, already made room for them.¹⁸

It is also worth noticing that the prosecutor's other major tool in this area, the continuing criminal enterprise statute, is considerably less flexible. When federal prosecutors charged the operator of the Silk Road marketplace, they relied in part on 21 U.S.C. § 848, related to drug-trafficking. That fits a single-operator marketplace with paid staff and would fit a cooperative of equals poorly. RICO's association-in-fact language is the more accommodating instrument.¹⁹

IV. THE PREDICATE GAP

If the enterprise element is not the difficulty, the list of predicates is. Racketeering activity under § 1961(1) covers wire fraud, access-device fraud, identity-document fraud, money laundering, extortion affecting commerce, criminal copyright infringement, and trade-secret theft, among many others.²⁰ A great deal of cybercrime falls within those headings. Phishing and business-email compromise are wire fraud. Selling stolen card numbers implicates the access-device statute. Moving the proceeds through mixers and exchanges is money laundering, and the money-laundering statute has the advantage of expressly reaching some conduct abroad.²¹

What the list does not contain is the Computer Fraud and Abuse Act's core provision on unauthorized access, 18 U.S.C. § 1030, or the general federal statute on interstate threats, 18 U.S.C. § 875.²² Congress has amended the list before when a new category of crime seemed to warrant it; the Defend Trade Secrets Act of 2016, for instance, added economic espionage and trade-secret theft.²³ No comparable amendment has been made for computer intrusion. The consequence is uneven. A crew that steals credentials and uses them to drain accounts will usually be chargeable through wire fraud or access-device fraud. A crew that breaks into networks to sell access, or that deploys ransomware and demands payment, may not fit so cleanly. The government can argue that a ransom demand is Hobbs Act extortion, since the statute reaches property obtained through "fear," and fear of economic loss from locked systems is at least arguable.²⁴ That theory must be proved case by case, and it does not cover an intrusion group whose only product is access or data.

¹⁷ Infraud Press Release, *supra* note 1.

¹⁸ See Susan W. Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, 4 N.C. J.L. & Tech. 1 (2002).

¹⁹ 21 U.S.C. § 848(c); see *United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017) (affirming conviction that included a continuing-criminal-enterprise count arising from the operation of the Silk Road marketplace).

²⁰ 18 U.S.C. § 1961(1)(B) (listing, among others, §§ 1028, 1029, 1343, 1951, 1956, 1957, 2319, and 2320).

²¹ *Id.* § 1956(f) (extending jurisdiction over certain conduct outside the United States).

²² Neither 18 U.S.C. § 1030 nor 18 U.S.C. § 875 appears in the list in *id.* § 1961(1).

²³ Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 3(b), 130 Stat. 376, 381 (amending 18 U.S.C. § 1961(1) to add §§ 1831 and 1832).

²⁴ 18 U.S.C. § 1951(b)(2) (defining extortion as "the obtaining of property from another, with his consent, induced by wrongful use of actual or threatened force, violence, or fear, or under color of official right").

The gap is not merely technical. It means that the statute's reach over an online network depends on which crimes its members happen to commit, and that the line between covered and uncovered conduct has little to do with seriousness. A group that sells a million stolen card numbers is within RICO's list; one that cripples a hospital's records system without taking money in a way that fits the fraud statutes may not be. The better response is legislative. Adding the felony provisions of § 1030 and the extortion provision of § 1030(a)(7) to § 1961(1) would align the list with the conduct that now defines the problem, and it would do so by the same method Congress has used for other categories of offence.

The objection to such an amendment deserves to be taken seriously, because RICO is a heavy instrument. A defendant charged under it faces enhanced penalties, forfeiture, and the reputational weight of the racketeering label. A hacker who compromises a handful of machines should not be described as a racketeer. Two safeguards answer much of this concern. The statute still requires an enterprise and a pattern, so a lone intruder is outside it. And the Department of Justice requires approval at the Criminal Division level before any RICO indictment or civil complaint is filed, which supplies a layer of institutional restraint that does not appear in the statute's text.²⁵

V. PATTERN AND CONTINUITY IN FAST-MOVING GROUPS

The second structural strain is continuity. In *H.J. Inc. v. Northwestern Bell Telephone Co.* For online groups this cuts in two directions. On the one hand, the infrastructure of cybercrime is built for repetition.²⁶ A marketplace that lists stolen goods every day, or a malware-as-a-service operation that licenses its product to affiliates, carries an obvious threat of ongoing activity, and the government can usually show it with server logs and sales records.²⁷ On the other hand, ransomware crews are known to dissolve,

rebrand, and reconstitute under new names, sometimes within months. A prosecutor who has evidence of only a single campaign by a short-lived crew may be unable to show a substantial closed period, and the group's habit of disappearing can undercut the argument for an open-ended threat. The enterprise's persistence across rebranding then becomes the central factual question, and the government's best evidence is usually continuity of personnel, code, wallets, and infrastructure.

Conspiracy charges soften the problem. A defendant charged under § 1962(d) need not personally commit two predicate acts.²⁸ That standard matters for the many participants in an online network whose role is technical or supportive, such as a developer, a host, or a laundering intermediary

VI. WHERE THE CRIME HAPPENS: DOMESTIC CONDUCT AND DOMESTIC INJURY

American courts begin from the presumption that "when a statute gives no clear indication of an extraterritorial application, it has none."²⁹ In *RJR Nabisco, Inc. v. European Community*, the Court applied that presumption to RICO and reached a split result. The substantive prohibitions of § 1962 can reach a pattern that includes foreign predicates, but only where each predicate statute itself applies abroad; the private right of action in § 1964(c), by contrast.

Two consequences follow for online groups. The first concerns predicates. The Second Circuit supports a racketeering charge only when the offence is committed domestically, and it has located the domestic component in the use of United States wires as a core feature of the scheme.³⁰ Where the scheme depends on transmissions into or out of the United States, in other words, a domestic violation may exist even if the operators sit overseas, and the Supreme Court has treated a wire-fraud scheme as a domestic offence when the defendants carried it out through

²⁵ U.S. Dep't of Just., Just. Manual § 9-110.101 (requiring prior approval of the Criminal Division before the filing of a RICO indictment, information, or civil complaint).

²⁶ *H.J. Inc.*, 492 U.S. at 239.

²⁷ *Id.* at 242.

²⁸ *Salinas v. United States*, 522 U.S. 52, 63–65 (1997).

²⁹ *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010).

³⁰ *Bascuñán v. Elsaca*, 927 F.3d 108 (2d Cir. 2019).

wires from within the United States.³¹ But a network that targets victims abroad, hosts its servers abroad, and merely routes some traffic through American infrastructure presents a thin domestic nexus, and courts will have to decide how much routing is enough. The answer is not settled. Money laundering gives the government a firmer footing, because Congress has expressly extended that offence to certain conduct abroad, including conduct by non-citizens that occurs “in part” in the United States where the transaction exceeds \$10,000.³²

The second consequence concerns civil plaintiffs. The domestic-injury rule was left undefined in *RJR Nabisco*, and the lower courts struggled with it, often asking where the plaintiff resided or where the funds sat. In *Yegiazaryan v. Smagin*, the decision gives cyber-victims some room. A company that suffers a loss through intrusion into its American systems, or a plaintiff whose property rights exist only under American law, has a plausible domestic injury.³³ A foreign firm defrauded abroad by a group that happened to use a United States email provider has a much weaker one. The Second Circuit’s earlier approach, which looked at where the property was located and the loss suffered rather than where the scheme began, points the same way.³⁴

VII. CIVIL PLAINTIFFS, CAUSATION, AND FORFEITURE

Even a plaintiff with a domestic injury must connect it to the violation.³⁵ The Court applies that principle strictly in later cases, rejecting claims where the harm to the plaintiff was derivative of a harm to someone else.³⁶ Data-breach litigation tests the rule in a familiar way. A bank that reimburses customers after card numbers are stolen may argue its loss was direct, but it will face the objection that the immediate victim was

the merchant whose system was breached. How far the direct-injury rule lets such claims travel is an open question.

Remedies on the criminal side raise a different difficulty. Section 1963 reaches interests acquired in violation of § 1962, interests in the enterprise, and “any property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from racketeering activity.”³⁷ The forfeiture provisions were designed with real property, businesses, and bank accounts in mind. Cryptocurrency held in wallets controlled by pseudonymous keys, and servers rented in foreign data centres, are a poor fit for traditional seizure mechanics, and the identification of which defendant controlled what is often the hardest evidentiary problem in the case. The Supreme Court’s decision in *Honeycutt v. United States*, which limited forfeiture under a parallel drug statute to property the defendant himself acquired, raises a further question for network cases in which proceeds flow to a few administrators and not to the many members who were charged.³⁸ Whether that reasoning carries over to § 1963(a)(3), whose wording is different, is a question on which reasonable courts could disagree.

VIII. COMPARATIVE NOTES

Other legal systems resolve this issue through different draftsmanship alternatives. Two of those alternatives provide guidance. The first alternative is the United Nations Convention Against Transnational Organized Crime.³⁹ The Convention defines an “organized criminal group” as a structured group of at least three individuals that exists for a specific amount of time, and acts collaboratively to engage in serious criminal activity to obtain a monetary or non-monetary

³¹ *Pasquantino v. United States*, 544 U.S. 349, 371 (2005).

³² 18 U.S.C. § 1956(f).

³³ *Yegiazaryan v. Smagin*, 599 U.S. 533 (2023).

³⁴ *See Bascuñán*, 927 F.3d 108.

³⁵ *Holmes v. Sec. Inv’r Prot. Corp.*, 503 U.S. 258, 268 (1992); *see* 18 U.S.C. § 1964(c).

³⁶ *See Anza v. Ideal Steel Supply Corp.*, 547 U.S. 451, 461 (2006); *Hemi Grp., LLC v. City of New York*, 559 U.S. 1, 9–10 (2010).

³⁷ 18 U.S.C. § 1963(a)(3).

³⁸ *Honeycutt v. United States*, 581 U.S. 443, 454 (2017).

³⁹ United Nations Convention Against Transnational Organized Crime art. 2(a), Nov. 15, 2000, 2225 U.N.T.S. 209.

benefit.⁴⁰ That language is strikingly close to Boyle, and it suggests that the supposed difficulty of fitting loose networks into an organised-crime definition has been recognised, and resolved, at the treaty level for some time. Its limitation is jurisdictional. The Convention applies to offences that are transnational in nature and involve an organised criminal group, and it relies on states to implement it through domestic law.⁴¹ A more recent instrument, the United Nations Convention against Cybercrime, adopted in December 2024 and opened for signature in Hanoi in October 2025, adds provisions on international cooperation and the sharing of electronic evidence, although it will not bind anyone until forty states have ratified it.⁴² The older Council of Europe Convention on Cybercrime remains the main operational framework for its parties.⁴³

The second comparison is domestic. India's Bharatiya Nyaya Sanhita of 2023 defines "organised crime" to include continuing unlawful activity such as kidnapping, extortion, economic offences, and "cyber-crimes," committed on behalf of an organised crime syndicate.⁴⁴ Where RICO uses a closed list of cross-referenced statutes, the Indian provision names cybercrime directly, and it defines a syndicate as a group of as few as two persons. That drafting is more compact and less likely to leave gaps of the kind identified in Part IV, but a broad, short definition also gives the prosecution wide latitude and invites overbreadth objections. Neither technique is plainly better. The comparison does show that the predicate gap in the American statute is a product of legislative method, not a necessary feature of racketeering law.

IX. CONCLUSION

RICO was not written for the internet, but the claim that it cannot cope with it does not survive a close reading. The enterprise concept, which many assume to be the obstacle, was loosened by the Supreme Court long before online forums existed, and the treaty.

Where the statute falters is at the margins that Congress itself drew: a predicate list that leaves out computer intrusion and some ransomware conduct, continuity doctrine that has to be applied to groups that vanish and reappear, and a set of geographic and causation limits that make civil enforcement uncertain for foreign and indirect victims.

None of these defects calls for judicial invention. The most direct repair is a short amendment adding the principal computer-intrusion and cyber-extortion offences to § 1961(1). The remaining problems call for careful charging, attention to evidence of continuity across rebranded groups, and continued internal review of when the racketeering label is warranted. Courts, for their part, will need to say more about how much domestic wire use makes a scheme domestic, a question that will keep recurring. A statute built to reach whoever organises crime, whatever form the organisation takes, can do this work, but only if its list of crimes keeps pace with the crimes being committed.

⁴⁰ *Id.* art. 2(c).

⁴¹ *Id.* art. 3(2).

⁴² G.A. Res. 79/243 (Dec. 24, 2024) (adopting the United Nations Convention against Cybercrime); United Nations Convention against Cybercrime art. 65(1).

⁴³ Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

⁴⁴ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, § 111(1) (India).