Convergence Focus Group: IUU Fishing and Banks

July 2024
Quantifind

Introduction

On July 16, 2024, Quantifind hosted a focus group on Illegal, Unreported, and Unregulated (IUU) Fishing with various ecosystem partners. The session aimed to explore how banks can more effectively contribute to the fight against illegal fishing. Financial Intelligence Units (FIUs) at banks are generally aware of this criminal activity and interested in aiding investigations that uncover and deter IUU fishing and related illicit activities. However, their experience varies widely, they face severe bandwidth constraints due to other risks, and their partner network in this space is limited.

The focus group enabled bank investigators to share best practices for illegal fishing investigations and level-set with their peers on how to best operationalize internal reviews and risk mitigation practices. It also fostered connections with new partners, including non-profits, technology providers, and government officials from both intelligence and law enforcement agencies.

This white paper summarizes the insights and recommendations gathered from this productive conversation.

Insights and Recommendations

Bank Motivations

Banks face a wide range of risks, and illegal fishing is only one of many priorities. Even within the ESG (environmental, social, governance) category, issues like illegal mining and wildlife trafficking often outrank IUU fishing due to higher volume and regulatory priorities. These risks are sometimes easier to trace back to responsible parties and often correlate with higher priority risks such as terrorist financing, offering a greater perceived return on investment for analysts. Additionally, as with many environmental crimes, the dollar amounts are often not extremely high for individual transactions, despite the large collective financial impact and the severe environmental impacts of the illicit activities.

Awareness of IUU fishing among banks varies. Some are more advanced in their technical approach to illegal fishing, and understand specific details, including vessel ownership chains and AIS (Automatic Identification System) tracking systems. Others are just becoming aware of the issue and consider it as a niche sub-component of an already niche Wildlife Trafficking risk.

During the session, participants suggested several ways to amplify the motivation and capabilities of banks, including:

- Tie the typology more directly to other convergent risks including **Labor Exploitation** (a.k.a., sea slavery), **Human Trafficking,** and **Drug Trafficking.**
- Highlight **national security risks** linked to the militaries or governments of Great Power competitors, including China. **Dual use** (military+commercial) indicators related to vessels are likely to increase priority.
- Make it technically easier to **de-anonymize the ultimate benefactors** by using data from partners to link the activity from vessel to owners to beneficiaries. The technical effort should also focus on disentangling the complicated web of actors involved beyond the stated owners (group owners, registered owners, operators, technical managers, etc.).
- Engage with **bank leadership,** which often plays a motivational role in choosing which missions or causes a particular bank emphasizes.
- Focus on cases with **large dollar activity** or high reputational risk.
- Banks should establish **common standards** for risk detection that consider both what **Oceana recently produced** for the insurance industry and the **Risk Cards** that Quantifind has produced for IUU fishing (among many other risks).

Tip Sourcing and Enrichment

While there are exceptions, tips or alerts for anomalous activities related to illegal fishing are mainly driven by law enforcement requests, and not the banks themselves. Wire data and financial transactions do not always tell a complete story, and it is very difficult to separate the proceeds of illegal fishing from legitimate activities from financial data alone.

Of course banks can, and should, follow negative news to find lagging indicators of related activity, but these are usually "after the fact". These signals should still be added to any comprehensive KYC screening process where customers are directly or indirectly (through relationships) linked to IUU fishing.

For leading signals, analysts at NGOs, tech companies, other financial institutions (e.g., insurance), and certain government groups are often in the best position to recognize illicit behaviors as they are happening. As with all investigations, the tips that are transferred between these organizations are most useful if they are enriched and labeled with as much connective metadata and identifiers as possible (company names, ultimate owners, summarized risks).

Law Enforcement Requests and 314A

No matter how good a tip is, the reality is that banks are more likely to prioritize investigative leads from law enforcement as opposed to an NGO or technology partner. Banks have limited resources and are better positioned to respond to direct law enforcement requests, in a process that provides them with proper insulation and legal authorities to reveal information.

The proper way to get banks to contribute to the illegal fishing solution is to create a "linear tip generation pipeline". This pipeline should start from observational partners (e.g., NGO's, companies, or government-based tracking systems, who consolidate raw data into events and entities of concern), whose alerts are potentially fed through other data partners for enrichment (e.g., connections to owners and other risks). Then, these partners can turn over relevant data to law enforcement partners, who determine whether the information passes their bar for investigation. If so, the law enforcement agency can then use legal mechanisms to file requests with banks to further adorn the case with financial transaction data.

This process is not unique to illegal fishing, and often uses 314A, part of the Patriot Act that allows law enforcement agencies to request information from financial institutions about individuals or entities that may be involved in financial crimes. (The 314B, in contrast, enables banks to share data with each other).

The agencies that would potentially relay information using this process include US FWS (Fish and Wildlife Service), HSI (Homeland Security Investigations), and the Department of Justice (DOJ, including FBI). Some of the requests may initially come in the form of other investigations, including drug trafficking. Other government groups, including NOAA (National Oceanic and Atmospheric Administration), the US Coast Guard, and the US Navy, are more disconnected from financial institutions but can play supportive roles throughout the pipeline, as mediated by the law enforcement agencies with appropriate authorities. This could either leverage existing sharing forums or have a dedicated 314A/B forum for IUU fishing cases.

(An issue not fully addressed here is what would motivate law enforcement themselves to prioritize IUU fishing cases higher than other cases, given their limited bandwidth. One cursory answer is that better tips through more established partnerships will help those agencies to dedicate resources to cases that would otherwise be ignored. Those tips can be improved by consideration of the red flags and other information presented in this report.)

Feedback Loops

Banks can also run the linear pipeline in reverse, allowing them to collaborate with law enforcement for better investigative outcomes. Banks should iterate with the law enforcement agencies to get all the data they need to provide the best possible investigative product from their data. Ideally, the resulting intelligence would combine signals of multiple crimes (illegal fishing and financial crimes) to give law enforcement the most leverage possible. This process should include active engagement between an outreach group at the financial institution and the requesting law enforcement agency, including phone calls and person-to-person engagement.

Red Flags

While it is difficult to discover unequivocal evidence of illegal fishing activity from bank data alone, there are certain patterns that banks can monitor, either by themselves or in collaboration with partners. This is not a comprehensive list but is representative of topics from the focus group conversation:

- **Crew Anomalies:** For the correlated risk of labor exploitation, where crews may be unwillingly kept captive for months at a time, certain anomalies may present themselves in bank data. For example, if the number of ships and payroll records (number of crew members) do not align, this can be indicative of an exploitative operation. Similar anomalies can also be monitored, including observed activity not matching stated purpose (or industry) and ships not returning to port.

- **Shell Companies:** Shell companies are common in the maritime industry, especially as they interact through certain regions and country registries (e.g., Panama, Liberia, Vanuatu, Marshall Islands, etc.). The presence of such obfuscating behavior alone is not necessarily a strong enough signal but in conjunction with other observations should be part of any investigative story.
- **Dual Use:** A primary goal, and often the most difficult task, of any fishing analysis is determining ultimate controllers and beneficiaries of the vessel. This extends not only to corporate parents but to nation states who support these activities. As discussed in the related Convergence session on **Adversarial Capital,** connections to Great Power competitors, including military organizations or state-owned entities from China, can further motivate action and incentivize allies to help support efforts to block actions.
- **Risk Regions:** Let alone other well known behavior (going dark, unusual rendezvous behavior), the simple presence of a vessel in particular narrow regions of interest is enough to trigger certain illegal fishing related risk factors.
- **Risky Vessel Types:** Longliners are known to be involved in IUU fishing more often than other vessel types.
- **Ports of Convenience:** Using port visit data, Global Fishing Watch has identified certain ports as risky. Visits to these "ports of convenience" should be considered in any relationship network and considered as a potential red flag.
- **Flags of Convenience:** Flags of Convenience (FOC) are used when a ship's owners register their ship in a country other than their own. As with shell companies, these are often used to evade detection and hide ultimate ownership. "Flag hopping" is a further signal of evasive behavior.
- **Satellite Enhancement:** Some risks come from a process by which vessel behavior triggers the tasking of satellite assets to examine the details of a ship for more anomalous behavior, either on the physical details of the ship itself or its encounters. E.g, a squid boat loitering on AIS and off loading to a refrigerator vessel that has gone dark. **Combined with other red flag signals,** these dark vessel interactions and transshipments become even more suspicious.
- **Blacklists:** Outside of international restrictions like sanctions, there are also more local blacklists of interest. For example, Regional Fisheries Management Organizations (RFMO) generate blacklists of vessels that should be considered in any risk analysis.

Data Sharing and Connectivity

Because even small investigations will include many nations, data partners, and investigative teams, an emphasis on data sharing and collaboration is essential. Here are several related recommendations from the focus group:

- **Usable Data:** For those data providers who have direct access to vessel tracking information, the form of the data that they productize, sell, and share with partners can be critical. On the one hand, overly raw data is not useful. On the other extreme, "overly baked" reports may not be necessary. In between, these providers can provide knowledge graphs representing non-obvious relationships between vessels and their respective owners. These relationships include rendezvous events between vessels including bunkerings (fuel supply), reefers (refrigerated cargo vessels) and transshipments, especially those where one or both vessels go dark from AIS tracking systems. By summarizing detailed information into consolidated events or risk signals, certain partners can help simplify the downstream analysis significantly.
- **Increased Collaborations:** The motivation for this focus group was that NGOs in the space currently have very limited interaction with financial institutions. Reinforcing these relationships, between those who observe and those who can act, should be an ongoing effort.
- **Battling Sparse Data:** When limiting an analysis to a single, small vessel it is very easy to hit a dead end. However, the key to de-anonymization is to connect the data to other ships or organizations that ultimately reveal insights. One way to do this is with certain data sets that directly connect vessels to owners or operators. These relationship networks can then be extended "up the chain" to ownership networks and relationships derived from news, transaction, or corporate databases that point to further relationship networks including shell companies and other means of obfuscation. Together these joint knowledge graphs can elucidate and demask illicit networks by combining assets from multiple organizations. Another way is to connect vessels to other vessels via their activity. Often small vessels interact with larger vessels (motherships or reefers/refrigerated vessels). As with all illicit trades or financial crimes, they have to integrate with legitimate actors at some point, and no market is completely dark. By increasing the knowledge graph integration points, these activities and connection points become more transparent. No one group sees a full network, only pieces. By recognizing all integration points, with data from different partners, the full story eventually becomes clear.

- **Graph Analysis:** In general, the same graph analysis approach should be taken as happens in other fields with intricate, multi-transaction criminal networks, e.g., drug trafficking. This points out the need for knowledge graph creation and visualization tools.
- **Foreign Language Focus:** Illegal fishing is an inherently international activity. Any analysis that does not include sufficient investigation and translation of foreign data (news, registrations, etc) will be incomplete. In particular, languages from Southeast Asia, Africa, and Latin America are of significant importance given the locus of activity, perpetrators, and victims.

Other Enforcement Pathways

The insights of this white paper are mostly biased towards US law enforcement workflows as they engage with financial institutions. However, there are several other intelligence-driven workflows that can also serve as part of the solution.

- While financial institutions are effective at screening existing customers for risks like illegal fishing and responding to law enforcement requests, they also have other means by which to limit the activities of bad actors in the space. Insurance providers are starting to effectively limit insurance policies for vessels based on illegal fishing related intelligence. Financing and leasing programs for vessels are also a potentially effective partner and consumer of such intelligence.
- Large commercial entities, such as restaurants and grocery chains represent the endpoint of the seafood supply chain and bear substantial responsibility and potential reputational risk. Investigative journalists have exposed several in bait-to-plate studies (e.g., **Outlaw Ocean**) that have been effective in raising awareness and prompting action.
- While the focus has been on law enforcement surgical actions, the force of sanctions also comes into play (via, e.g., State Department or Treasury) and these organizations should use illegal fishing related intelligence to amplify and extend more narrow sanctions to larger clusters and beneficial ownership networks of bad actors. US-led sanctions can continue to serve as a signal to sanctioning entities in foreign nations who can further limit illicit behavior.
- **Withhold Release Orders** (WRO) from US Customs and Border Protection (CBP) are another avenue through which illegal fishing concerns can come to the attention of a financial institution.
- Other countries, including the victims of illegal fishing activities, are also engaged in the fight often with US support. **Port officers** can use intelligence to better direct their inspection questions. Similarly, **onboard observers** can be better informed. Countries can also use shared data to better make decisions on which vessels are allowed to use their **flags of convenience (FOC),** as this is yet another obfuscation method that certain organizations use to hide their true identities.

Concluding Notes

A final recommendation for combating illegal fishing is for all participants to continue participating in events like this or any similar focus group. Sharing best practices is also a best practice. Public-private partnerships will remain critical for effectively collaborating, either informally or formally, through workflows that result in bad actors being detected and inhibited by proper legal authorities.

If you or your organization would like to be included in any potential follow ups for this working group, please reach out to **convergence@quantifind.com**.

Upon request, Quantifind can also share a detailed “Risk Card” for Illegal Fishing that details critical data sets, red flags, organizations, and training data, providing a comprehensive resource for any technical organization looking to participate in the solution. These standards are critical in training AI algorithms that address the vast scale of external, open-source data which should fuel any collaborative investigative effort.

For an introduction to the problem of IUU fishing, please see the book: **The Last Fish Swimming**.

Finally, the authors would like to thank **Oceankind**, the **Joint Analytical Cell**, and all of the focus group participants for their contributions and support.

QUANTIFIND
THE RISK INTELLIGENCE COMPANY