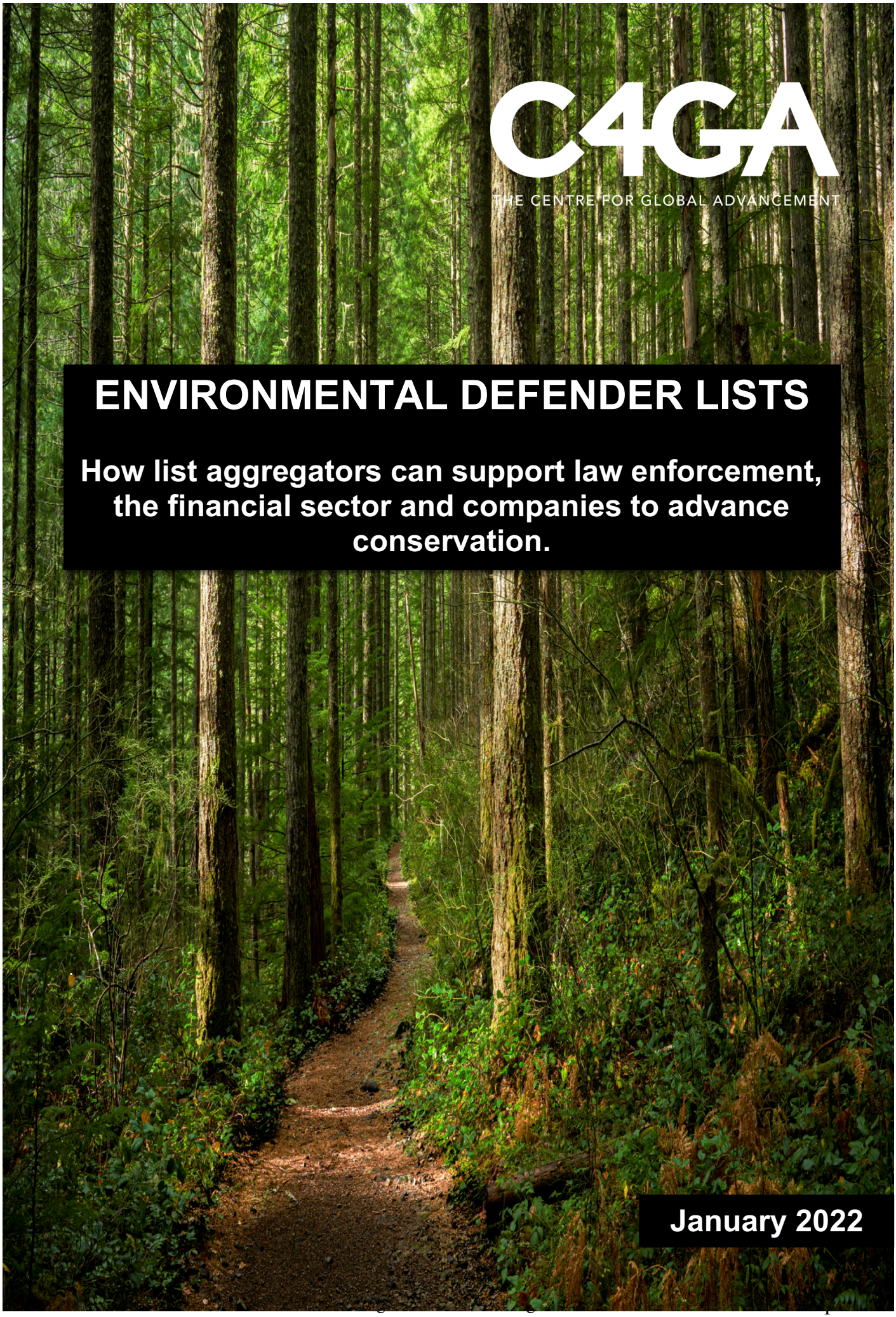

ENVIRONMENTAL DEFENDER LISTS

How list aggregators can support law enforcement, the financial sector and companies to advance conservation.

January 2022

Prepared by the Centre for Global Advancement
Author: Amanda Gore
January 2022

Acknowledgements
The Centre for Global Advancement (C4GA) is an organisation established to support alternative legal and financial pathways to combat environmental crime. This document was produced with support from the World Wildlife Fund (WWF). We express gratitude for the support and leadership to advance knowledge on how data can be used in a more connected way to combat environmental crime. We also express gratitude and acknowledgement to those list aggregators and other stakeholders that spent time to discuss their work and how they function.

Suggested Citation: Amanda Gore, "*Environmental Defender Lists: How list aggregators can support law enforcement, the financial sector and companies to advance conservation,"* Centre for Global Advancement, January 2022.

Table of Contents

Summary of Key Points

1. **LEVERAGE EXISTING DATA PLATFORMS**

⇒ Support the Environmental Investigation Agency (EIA) Media Monitoring Programme that collates data on environmental offenders for action by other list aggregators and key stakeholders to support law enforcement.

⇒ Promote existing **WHISTLE-BLOWING** platforms like Wildleaks and the Crime-stoppers International app as a mechanism for the public to report environmental harms.

⇒ Promote Collaboration between NGOs and list aggregators (Refinitiv, LexisNexis etc) to boost data on environmental offenders to encourage and flag more law enforcement investigations.

2. Understand the **LEGAL CHALLENGES** involved in sharing data on environmental offenders.

3. Understand the role that **INFORMATION-SHARING PLATFORMS** can play in supporting law enforcement actions (i.e.: United for Wildlife Transport and Financial Taskforces and formal Government-led financial crime forums (public-private partnerships)).

4. Map **PRE-DEAL DUE DILIGENCE** processes conducted by investors, financiers and companies. What due diligence tools are currently provided by list aggregators and are these tools adequate and "fit for purpose" to combat environmental crime?

5. Most importantly, consider **PROACTIVE** due diligence measures as part of investment, financial and business decisions to prevent further environmental harms. Keeping in mind that law enforcement actions takes place after an environmental crime event has already taken place.

6. Consider how watchlists and/or sanctions lists maintained by list aggregators could be more effectively leveraged to combat environmental crime.

Environmental Human Rights Defenders are defined as:
"individuals and groups who, in their personal or professional capacity and in a peaceful manner, strive to protect and promote human rights relating to the environment, including water, air, land, flora and fauna and promote human rights relating to the environment, including water, air, land, flora and fauna".

List Aggregators are organisations that collate data into one place for further analysis by third parties. (i.e.: Refinitiv, LexisNexis)

Executive Summary

Environmental offenders include individuals or companies that may be involved in environmental crimes including the illegal wildlife trade, deforestation and illegal logging, fisheries crime, illegal mining, waste trafficking and pollution crimes. Data on environmental crime offenders including individuals, and companies, is collated by list aggregators that maintain data and lists about various types of wrongdoers. These lists inform law enforcement, financial institutions, and companies to support law enforcement investigations as well as assisting banks to conduct due diligence and companies to make informed business decisions.

With increasing regulatory burdens, there is an acute need for easily accessible data to perform due diligence services prior to making business decisions. Within banks and companies, it is now standard practice to incorporate pre-deal due diligence services to ensure that services and financing are not extended to bad actors linked to various crimes. This report seeks to understand how list aggregator services can contribute to combatting environmental or “green crimes” by harnessing data that exists on entities involved in environmental crimes.

The key findings of the report show that list aggregators can support work to combat green crimes in two ways:

1. **Supporting law enforcement** investigations linked to environmental crime by providing data that may show potential or established unlawful activities. Law enforcement investigations are reactive and take place after an environmental crime event has occurred that might result in a prosecution action, various sanctions, fines, or penalties. List aggregator services also support financial investigations linked to environmental crime undertaken by banks and financial institutions that may report suspicious activity for further law enforcement action

2. **To conduct proactive due diligence** related to company purchasing and supply decisions including wider supply chain risks linked to third party suppliers. Proactive due diligence will also be used before financing is extended, new business relationships established, or investments are made by various companies and financial institutions.

Initiatives to collect and share data on environmental offenders have traditionally been targeted at law enforcement actions. This report highlights how list aggregators and data can play a key facilitating role in proactive due diligence processes and ensuring that those entities linked to environmental crimes are penalised through the re-evaluation and/or cessation of business relationships across supply chains, cutting off financing or influencing companies to comply and stop engaging in environmental harm.

Introduction

Applying financial crime tools and techniques to environmental crimes has recently become a significant focus of policy and decision makers as a potential avenue to disrupt activities linked to environmental crime. Environmental crimes are inextricably linked to financial crimes including corruption, money laundering, tax offences and fraud, and often human rights abuses are also part of the complexities of investigations linked to environmental crime issues. On 6 December 2020, the European Union ("EU") introduced the 6th Anti-Money Laundering Directive ("6AMLD") which now includes environmental crime as a predicate offence. This has prompted action from a number of European countries along with list aggregators that are now focused on understanding data and information on environmental crime and environmental offenders. This new directive makes it a requirement in the European Union to understand money flows linked to environmental crimes which has prompted action from list aggregators to build additional capacity and collect data on environmental offenders to meet this demand.

With multiple lists aggregated by the data providers, sanctions lists are by far the most prevalent where clients screen their potential clients against sanctioned entities. OFAC SDN[1] listings issued by the US Treasury restrict US citizens and residents from doing business with these designated entities and usually reserved for most egregious offenders. A recent sanctions example linked to mining is Mr. Dan Gertler who was placed on an OFAC Sanctions list in 2017 for engaging in human rights abuses and corruption linked to his mining operations in the Democratic Republic of Congo (DRC)[2]. This sanction occurred under Executive Order 13818 signed on December 20, 2017 [3]and resulted in assets within U.S. jurisdiction being blocked, and U.S. persons being prohibited from engaging in transactions with him. Further watchlists are also maintained by various government, enforcement and regulatory agencies to combat various types of crime. These additional watchlists could potentially be leveraged for environmental offenders that are linked to other crimes, and banks could also consider creating internal watchlists to monitor potential environmental offenders.

[1] OFAC– the Office of Foreign Assets and Control, https://sanctionssearch.ofac.treas.gov/ and SDN – Specially Designated Nationals and Blocked Persons Lists.
[2] US Treasury OFAC listing https://home.treasury.gov/news/press-releases/sm0417
[3] The Daily Journal of the United States, Executive Order 13818, *"Blocking the Property of Persons Involved in Serious Human Rights Abuse or Corruption*", 26 December 2017 https://www.federalregister.gov/documents/2017/12/26/2017-27925/blocking-the-property-of-persons-involved-in-serious-human-rights-abuse-or-corruption

Methodology

The report has been prepared based on a desk review of list aggregators combined with surveys and interviews of industry players. This includes interviews with banks and financial institutions, list aggregators, non-profit organisations and researchers that collect and share data on environmental crime matters. In addition, this report has drawn heavily on personal experiences at non-profit organisations, banks and law enforcement agencies and the due diligence processes undertaken with the use of list aggregation services.

Section 1: List Aggregators

There are many market data providers providing list aggregation services that identify sanctioned individuals and other high-risk designated persons. These list aggregators provide paid data and analytic services that can be used for compliance, due diligence or investigative purposes. Historically, these list aggregation services have been used as part of law enforcement investigations with a financial crime and sanctions focus however there is now a wide range of data tools including access to data that will help evaluate the performance of a company based on Environmental, Social and Governance (ESG) indicators. This data can support decision makers to conduct up-front due diligence on their supply chain partners, investments and with due diligence responsibilities before extending finance and entering deals.

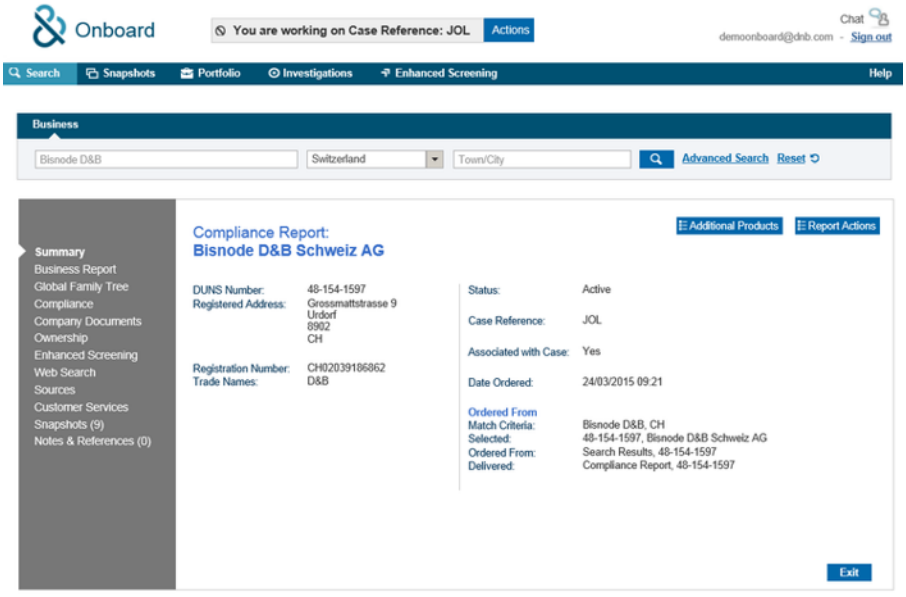

Figure 1: Dun & Bradstreet Company Search Interface

1.1 Supporting Law Enforcement Action

A review of key list aggregators Refinitiv, LexisNexis, Dun and Bradstreet and Bureau van Dijk (Moody's) has been conducted for their input into collecting data on environmental offenders. Standard data is collected by each company and made available through a single search function and often includes: public

records data and company registration details, company family tree and connected entities, politically exposed persons (PEP), close associates, and family members, global sanctions lists, global regulatory and law enforcement lists, adverse media, ultimate beneficial owner (UBO) and in some cases vessel information where vessels may be designated or sanctioned.

Figure 2: Data Inputs reported by LexisNexis

Lexis Nexis reports the following data inputs:

- **State Owned Enterprises**: A list of government-owned and government-linked corporations and businesses, as well as senior employees of those entities.
- **Politically Exposed Persons:** A database of Politically Exposed Persons ("PEPs"), as well as those of their family members and associates
- **Adverse Media:** An extensive database of profiles that have been linked to illicit activities from over 30,000 news feeds worldwide
- **Sanctions Lists:** Information from the most important sanction lists worldwide, including OFAC, EU, UN and HMT. Our OFAC sanctioned lists cover entities with 10% or more ownership.
- **Entities associated with sanctions:** Family members and associates of sanctioned entities, branches and operational units of sanctioned banks and entities owned or controlled by subjects sanctioned by OFAC, the European Union or HMT.
- **Enforcement Actions**: Information from over 1,600 enforcement sources worldwide, such as the FDA, HHS, SEC, FBI and UK FCA
- **Registration Data**: Concentrated coverage of registration lists focused on specific risk and compliance issues built from various government sources

Source: https://risk.lexisnexis.com/global/en/financial-services/financial-crime-compliance/watchlist-screening

Refinitiv, a list aggregator that provides a number of data products has created a relatively high profile with respect to their "green crime" programme[4] focusing on environmental crime[5] The company has been active in encouraging NGO partnerships with an environmental focus to harness more targeted data linked to environmental offenders to inform its end-user clients. List aggregators are often limited by imposing a requirement that data be verified through a *reputable public source*[6], thereby limiting the scope of data that might be collected. The

[4] Refinitiv Green Crime Awareness Raising: https://www.refinitiv.com/perspectives/financial-crime/the-rise-of-green-crime-the-hidden-threat/

[5] Crimes included in the Refinitiv World-Check database: • Bribery and corruption • Hostage taking • Kidnapping • Piracy, counterfeiting and piracy of products • Human trafficking and other human rights abuses • Organized crime • Currency counterfeiting • Illicit trafficking in stolen and other goods • Racketeering • Cybercrime • Hacking • Phishing • Insider trading and market manipulation • Robbery • Environmental crimes • Migrant smuggling • Slave labor • Securities fraud • Extortion • Sexual exploitation of children • Money laundering • Falsifying information on official documents • Narcotics and arms trafficking • Smuggling • Forgery • Price fixing • Illegal cartel formation • Antitrust violations • Terrorism • Terror financing • Fraud • Embezzlement • Theft • Cheating • Pharmaceutical product trafficking • Illegal distribution • Illegal production • Banned/fake medicines • War crimes • Tax evasion • Tax fraud. As well as subjects convicted of these crimes, World-Check lists subjects who have been accused, investigated, arrested, charged, indicted, detained, questioned or placed on trial in connection with one or more of them. This distinction is always made clear.

[6] A reputable public source is defined through evaluation of the the news outlet or public based source. For example: BBC may be evaluated as a reputable source, where as a blog post or social media would not generally be acknowledged as a reputable public source.

internal research team at Refinitiv, however, works with NGOs to conduct follow up research on data leads to find a public source for otherwise non-public information to help ensure the data can be included within the service.

Case Study: Turning Intelligence into Actionable Data (Partnering with NGOs)
NGO X is a non-profit organisation based in Washington DC. The organisation was co-founded by Mr X and investigates "dirty money" linked to war crimes. NGO X has entered a partnership with Refinitiv to share information on those ***individuals or companies*** involved in war crimes and illicit financial flows. The Refinitiv research team will look for a verifiable public source to convert intelligence data into data that can be used in the platforms for their clients. This model could be applied easily to environmental NGOs to supply information and data on environmental offenders.

Figure 3: Broadening the data collection of environmental offender data

Within list aggregators, environmental data may appear in the following ways: adverse media, legal actions or if the company has been involved in other linked crimes, they may appear on one of the thousands of watchlists within the system. For example: Korean company Korindo will likely appear showing media articles linked to its termination from the FSC for environmental issues and human rights issues (see media article).[7] If there are legal actions linked to the company these will also likely appear within the search function. Figure 4 detailed below shows a graphic from Lexis Nexis around the actions they are taking to combat the illegal wildlife trade.

Figure 4: A graphic on the illegal wildlife trade from LexisNexis

Lexis Nexis and Bureau Van Dijk (Moody's) have both considered environmental crime issues. Bureau Van Dijk is actively developing their environmental portfolio as a response to the new European regulation 6AMLD[8]. Both list aggregators have published information linked to the illegal wildlife

[7] Hans Nicholas Jong, *"FSC dumps palm oil giant Korindo amid rights, environmental issues in Papua,"* Mongabay, July 2021 https://news.mongabay.com/2021/07/fsc-dumps-palm-oil-giant-korindo-amid-rights-environmental-issues-in-papua/
[8] 6AMLD - 6th Anti-Money Laundering Directive under the European Union

trade but not yet on broader environmental crimes. However, both LexisNexis and Refinitiv are receiving monthly data updates from their media monitoring programme on environmental offenders from the Environmental Investigation Agency (EIA) that are uploaded into their systems (more detail around the EIA Environmental Crime list is discussed in Section 2). As a point of comparison, the table below details the data inputs collected by the list aggregators of interest for the research.

Figure 5: Overview of data sources detailed by list aggregator

Financial Market Data Provider	Product Offering	Data sources
Refinitiv	World Check Risk Intelligence Enhanced Due Diligence	Around 35 percent of World-Check data is derived from information on sanctions, watch lists, or regulatory and law enforcement lists. The remaining 65 percent consists of information on PEPs (politically exposed persons), plus material on individuals and entities who are not on official lists but who are reported to be connected to sanctioned parties or to have been investigated for, or convicted of, financial crime, slavery or human abuse-related activities. World-Check provides the media sources upon which all such information is based.[9]
Lexis Nexis	Nexis Diligence Nexis Entity Insight	Lexis Diligence enables the monitoring of third parties with marketing intelligence that includes sanctions, watchlists, Politically Exposed Persons (PEPs) lists, Experian® business data, global news, and more.
Dun & Bradstreet	Third party risk and compliance tools	Compliance screening for watchlists & sanctions, PEP, or adverse media for reputational risk, beneficial ownership and onboarding (corporate structures, verification of incorporation and associated public records)
Bureau Van Dijk	Compliance and Financial Crime (Compliance Catalyst)[10]	Company information and corporate structures combined with sanctions and other adverse data. It also includes curated risk data from Grid, a risk database of adverse media, sanctions, watchlists and PEPs.

List aggregators can provide a more holistic picture of an entity (individual or company) linking multiple data sources all within one search. For example: a search on BP would show a link to the BP Deepwater Horizon Oil Spill in 2010 which would show government actions, adverse media, corporate structures, and other data. An individual involved in the illegal wildlife trade like Vixay Keosavang who has a $1m bounty placed on him from the US Government

[9] Refinitiv Website and Marketing Materials https://www.refinitiv.com/content/dam/marketing/en_us/documents/brochures/world-check-risk-intelligence-brochure.pdf
[10] Compliance Catalyst data.- https://www.bvdinfo.com/en-gb/solutions-for-your-role/compliance-and-financial-crime

would show adverse media results showing he is a person of interest "POI" to the US authorities and other linked companies globally. Finally, the Fisheries Ministers Bernhardt Esau and Justice Minister Sacky Shanghala in Namibia were accused to accepting bribes from Icelandic company Samherji for fisheries quotas in Namibia (the "Fishrot case"), the list aggregator would reveal the current allegations, adverse media, linked companies and previous legal history of the pair.

2.1 Sanctions and other Denied/Restricted person lists

In addition to comprehensive media, legal, public documents and corporate records, list aggregators maintain several watchlists that are screened as part of one single search. One list aggregator suggested that 2000-3000 lists exist within the current landscape and that the same lists are maintained across the industry.[11] These lists are generally sanctions lists with a heavy focus on terrorism-related crimes and updated by the UK, EU, US, Australia amongst other countries. The lists also include the FBI Ten Most Wanted, Interpol Most Wanted Fugitives, the World Bank Debarred Parties List and ICE Lists (U.S. Immigrations and Customs Enforcement) for example.[12] FINCEN also maintain lists, one in particular that is maintained in under Section 311 of the Patriot Act which designates a country, financial institution or international transaction of primary money laundering concern.[13] List aggregators monitor sanctions, regulatory and enforcement lists regularly, often daily, as well as thousands of reputable media sources to ensure accurate and up-to-date information. *(Refer to Appendix 1 for an example of sanctions and denied party lists from TRACE International).* Further interviews with entities that maintain watchlists are recommended to understand what information and/or evidence is required to list a company, individual or country on such a watchlist and if this could include environmental offenders linked to money laundering and other crimes.

2.1 Proactive Due Diligence

There are also list aggregator services and data tools that can be more effectively leveraged to support due diligence processes linked to Environmental Social and Governance (ESG) obligations. Conducting up-front due diligence before extending purchasing commitments, finance or investing into companies can assist decision-makers to prevent additional environmental harm by informing the financier, investor, or company of potential wrongdoing prior to entering any business relationship. In the ESG space, different list aggregators seem to be used more exclusively including MSCI,[14] Sustainalytics[15], TRACE International[16], Integrated Biodiversity Assessment Tool (IBAT)[17] and Rep Risk.[18] However, some providers like Refinitiv offer both

[11] Interview with list aggregator
[12] Refer Appendix 1 and LexisNexis https://risk.lexisnexis.co.uk/products/worldcompliance-data
[13] https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures
[14] Morgan Stanley Capital International (MSCI) https://www.msci.com/
[15] Sustainalytics Website https://www.sustainalytics.com/esg-data
[16] Trace International Website https://www.traceinternational.org/due-diligence-risk-assessment
[17] IBAT - Integrated Biodiversity Assessment Tool- https://www.ibat-alliance.org/
[18] Rep Risk https://www.reprisk.com/

ESG and Financial Crime Compliance data in separate product suites. Proactive due diligence can be used by companies to evaluate their global supply chains, banks and financial institutions around financing and organisations involved in investing in corporations that may be linked to environmental crimes. These providers are outside of the scope of the current research however it is recommended further work is conducted to map the ESG data landscape.

Section 2: Sources of Environmental Crime Data

List aggregators obtain information from multiple sources which is then consolidated and presented within a searchable systems database. With limited data on the environment captured in these systems to date, this section offers new avenues to encourage further data collection with respect to environmental offenders primarily through the EIA Environmental Crime Media Monitoring Programme and secondly by identifying broader data that may be accessible. Information sharing partnerships also collate data on environmental offenders. These partnerships will be examined for the potential data availability and collection in Section 3.

2.1 The EIA Media Monitoring Programme

The Environmental Investigation Agency (EIA) has taken ownership of a list originally compiled by Liberty Asia (now Liberty Shared) which collects data across the NGO landscape on offenders involved in the illegal wildlife trade, illegal logging, and some fisheries crimes (trafficking of shark fin and abalone for example.) This list captures data from various NGOs including monthly from TRAFFIC, provided it meets the following criteria:

1 There is a law enforcement action,
2 There is a named offender (forename and surname) or a named company; and,
3 An open-source URL reference for the recipient companies is available from a reputable source (not from social media).

EIA Data Aggregation – Environmental Crime Media Monitoring Programme
The Environmental Investigation Agency (EIA) compiles information on environmental offenders through a collaborative NGO forum and monitoring a wide range of media sources to be uploaded into the Refinitiv databases and other list aggregator services like LexisNexis.

For example: A potential IWT suspect, Mr Ansoumane Doumbouya, a Guinean and the CITES Management Official in Guinea, is involved in wildlife trafficking by providing falsified CITES permits to facilitate the trade in illegally sourced chimpanzees or gorillas. To include this data within the dataset, there must be a public source that shows there is a law enforcement action and it must contain the full name of the offender. In this case, BBC released a documentary on this investigation which is publicly available. If the information does not have a public source, it may be unable to be included.

Figure 6: EIA Environmental Crime Watchlist

2.2 Broader Collection of Data

The EIA Environmental Crime Media Monitoring Programme has the potential to aggregate a wider range of data for dissemination to list aggregators and other information-sharing platforms by creating new partnerships with a variety of NGOs to collect data. Wider data collection could also include a new layer of data from EIA public intelligence reports and other non-public intelligence data. This intelligence data could, subject to legal advice, be shared across existing information sharing platforms (discussed in Section 3) where it does not meet the standards of list aggregators (i.e.: have a public source) or alternatively in confidential bank briefings (again subject to legal advice). Further data could also be collected from court records. The EIA list currently includes court records on an ad-hoc basis but only where a URL exists.

<u>The EIA Environmental Crime Media Monitoring Programme has the potential to:</u>

- **Widen the scope of data collected** on environmental offenders (i.e.: including illegal mining data, fisheries crime, waste and pollution crimes for example)
- **Widen the channels to disseminate the data** by increasing the number of list aggregators or organisations that it sends data to for action.
- **Increase the number of partnerships** with NGOs and other partners to collect more data inputs on environmental offenders.

2.3 Limitations of Data Collection

Data privacy laws and the threat of defamation lawsuits are a constant challenge to those that collect data on environmental or financial crime offenders. For example: if a target of interest is included in a paid database service in a negative way, this could be a potential lawsuit for defamation if the information is not based on solid facts, hence the requirement for a public source. Data inputs on offenders must be from a "verified" source which means it is from a reputable source – i.e., a well-known and regarded news or media

outlet that is known for honest reporting or recognised government restricted lists. If there is an article on the BBC news highlighting the issues of deforestation linked to a Korean company, then the information on Korindo would be included in the lists as part of the adverse media section. e.g., Korindo in Indonesia (not a blog or social media post)

Section 3: Information Sharing Partnerships

Public-Private Partnerships (PPPs), also known as information-sharing partnerships have also become popular in the last 4-5 years across the financial crime landscape to trigger new investigations linked to the illegal wildlife trade and broader environmental crimes. The United for Wildlife Taskforces, based in the UK, are focused on sharing data and information on wildlife crime offenders obtained through public sources to the private sector (airlines, shipping lines and financial institutions) to create active new investigations to combat the illegal wildlife trade. The objective of this section is to highlight existing information sharing partnerships and examine these as potential data collection avenues that could be collated into mainstream list aggregators.

3.1 The United for Wildlife ("UfW") Taskforces

The United for Wildlife (UfW) initiative[19] was set up by the Duke of Cambridge with the launch of a "transport taskforce" that took place in 2014 with the Buckingham Palace Declaration followed by the launch of a "financial taskforce" under the Mansion House Declaration in 2019. These taskforce structures are aimed at providing collaborative working relationships between the private and public sectors to combat the illegal wildlife trade. The private sector members sign a declaration committing to combatting the illegal wildlife trade[20] as part of the business-as-usual operations.

The Transport Taskforce

The transport taskforce was created as a public-private information sharing partnership bringing together airport and customs personnel, shipping companies and airlines in a forum to share data and information on potential illegal wildlife trade movements globally. The transport taskforce is actively intercepting the trafficking of protected species through its networks of airlines, law enforcement and customs officials.

⇒ The transport taskforce has partnered with *Crime-Stoppers International,*[21] a non-profit organisation focused on supporting law enforcement, where people can report wildlife crime anonymously via an app. This information is then passed onto the taskforce for potential action and interception of trafficking events.[22]

[19] United for Wildlife Website - https://unitedforwildlife.org/about-us/
[20] IWT in a broader sense including illegal logging and some fisheries crime
[21] Crime-Stoppers International Website - https://csiworld.org/
[22] TRAFFIC, November 2021 "New mobile app is helping to combat corruption and wildlife trafficking" https://www.traffic.org/news/new-mobile-reporting-app-is-helping-combat-corruption-and-wildlife-trafficking-in-the-aviation-industry/

⇒ The transport taskforce is also working closely to share information with the financial taskforce, explained below, that seeks to trigger financial investigations linked to the illegal wildlife trade.

The Financial Taskforce

The financial taskforce brings together banks and financial institutions, money exchange services and mobile money providers to combat the illegal wildlife trade. The taskforce members receive regular intelligence alerts based on open source data identified by the UfW Secretariat that can be actioned by the financial service providers.[23] The taskforce is currently restricted to sharing publicly available information however they aspire to share further information and compile blacklists if the legal advice is favourable to do so. This could broaden the type of data collected and support a list-based approach that could also be utilised by list aggregators for a wider distribution of data linked to environmental offending.

Scope of Work	Successes	Limitations	Potential for advancement
IWT - species crime, illegal logging and selected fisheries (i.e.: trafficking of shark fin, abalone etc.)	High profile due to involvement of Prince William (UK). There are several global signatories both in the transport sector and financial sector who wish to be associated with the initiative to combat IWT. South Africa has been leading efforts to collaborate between the Government and UfW bringing together law enforcement with non-profit data. Real-time action and monitoring of bank accounts can take place on offenders.	Data collection is focused on law enforcement and "pure" wildlife crime, not a wider range of environmental issues. Can only technically deal in public information but legal advice is being sought to extend this.	Legal advice is being sought around the creation of IWT **blacklists**. Potential to enhance data sharing elements and actions between private and public sector.

Figure 7: Analysis of the successes and limitations of the taskforces

The scope of the current data collection is limited to the broader illegal wildlife trade including illegal logging, forest and fisheries crime, however harnessing this data within a list aggregator system could inform global stakeholders of the risks of doing business with those linked to wildlife crime and would be especially useful if these platforms can share "blacklists" created with list aggregators.

3.2 Formal Data Sharing Partnerships (i.e.: SAMLIT) led by Government

The South African Anti-Money Laundering Integrated Task Force (SAMLIT) is a new collaboration between the South African Government and the financial sector. The UfW financial taskforce has also been extremely active in South Africa in collaboration with the SAMLIT and shares data on IWT offenders which can lead to the routine tracking of bank accounts, cash deposits and maintaining watch lists of known associates potentially involved in the illegal wildlife trade. This SAMLIT model compels the private sector banks to act on confidential government information and to conduct investigations to combat IWT and other financial crimes.

3.3 Whistleblowing Platforms - Wildleaks

Wildleaks was launched around six years ago and aimed to be an anonymous platform for people to report broader wildlife and environmental crime for action by authorities globally. The first Wildleaks report was launched online in September 2020 and reveals 300 reports or "leaks" that have been received along with example case studies.[24] The platform has suffered from an initial lack of resources to promote and develop the platform to its full capacity. Some of the early challenges have included getting local law enforcement to act on the leaks obtained, especially in less developed countries. The platform is focused on law enforcement action for a range of wildlife crime offences however it also targets broader environmental crime. Wildleaks could be another potential source of data on environmental offenders that could be leveraged by list aggregators. A summary of the successes and limitations are detailed below:

Scope of Work	Successes	Limitations	Potential for advancement
Wildlife Crime – including forestry and fisheries crime. Potential to capture more data.	300 reports to the whistleblowing platform with a series of case studies reported.	Concerns that the information will arrive in the right place for action and that the information will be actioned at all.	Broadening of the scope and awareness of the platform. Awareness raising on whistle-blower rewards to encourage additional information.

Figure 8: Analysis of the successes and limitations of the whistleblowing platform

[24] Wildleaks Report, September 2020 - https://wildleaks.org/wp-content/uploads/2020/09/WildLeaks-Report-Sept2020.pdf

Section 4: The Role of Banking and the Financial Sector

Banks and financial institutions can play a key role in combatting environmental crime. They primarily act as a law enforcement agent reporting suspicious activity and transactions under Anti-Money Laundering ("AML") legislation. Investigations into environmental crimes are often triggered by adverse media or tip-offs from NGOs, supported by list aggregator services to understand the big picture of the client. Secondly, banks are required to conduct due diligence on clients that require finance. List aggregators can support up-front due diligence and identify potential risks with the client. With allegations of linkages to environmental crime, banks can play a key role in cutting off finance or influencing the company to put policies in place, make declarations or put conditions on loans that ensure that the company will not be involved in environmental criminal activity.

4.1 Law Enforcement Action

Banks receive information from several sources including list aggregator data to comply with their AML and due diligence obligations. Banks also maintain internal watchlists as well as complying with government mandated blacklists. Automated transaction monitoring systems are used to flag high-risk transactions or completely block transactions linked to undesirable clients and counterparties. If there are concerns on a client and/or counterparty, the bank conducts an internal investigation and is required to report a suspicious transaction report ("STR") or suspicious activity report ("SAR") if there are sufficient suspicions linked to the transaction or client.

This STR is sent to the national financial intelligence unit ("FIU") established in most countries globally which is then further investigated. Further data is collated by the FIU before it is referred to one or multiple law enforcement agencies for further investigation. Law enforcement agencies that receive these reports can include: the tax and revenue authority, the national police, the anti-corruption agency or any other relevant law enforcement agency that may need to take action. Within the national AML legislation, it is mandated who must report STRs, this differs per country but can also include lawyers, accountants, casinos, used car yards for example depending on the national laws. NGOs are not usually mandated to report STRs hence they often work with banks to help trigger investigations on environmental targets of interest.

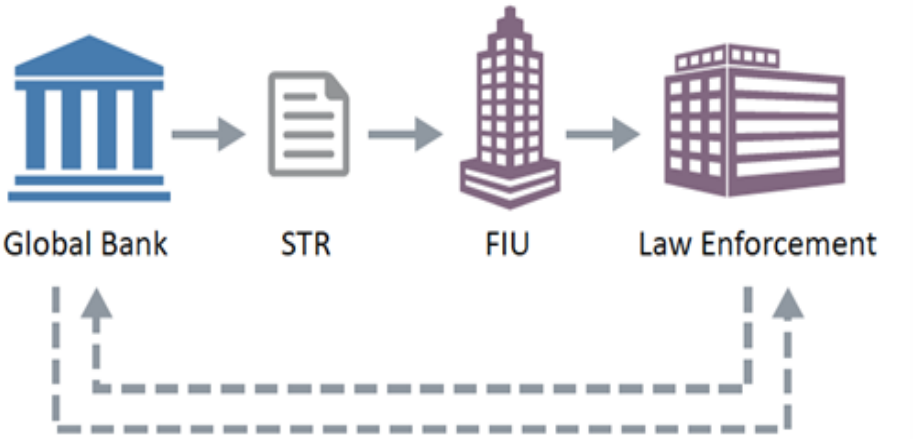

Figure 9: The law enforcement process

Law Enforcement Investigation – Sanitised Case Study
A global bank receives information from an NGO that "XYZ Pet Store" in Singapore (fictional name) is involved in purchasing falsifying CITES permits from a CITES Management official in West Africa. The bank then investigates "XYZ Pet Store" and identifies payments of US$5,000 to Mr. D the CITES Management official in Guinea which reveals itself to be a bribe payment for a falsified CITES permit. This transaction would require a Suspicious Transaction Report (STR) to be filed in Singapore and this information would then be passed onto Singaporean Police or another relevant law enforcement agency for further investigation of the Pet Store. Similar law enforcement action would need to be reported in the West African country for the allegedly corrupt government official.

A US-based consortium recently compiled a list of alleged environmental offenders and shared this data with several global multi-national banks for further financial investigation and reporting of STRs where there was evidence of wrongdoing. Banks are often reliant on third parties and NGOs to share data on environmental offenders to trigger new financial investigations and are often open to receiving intelligence data due to the lack of actionable offender data sources. List aggregators often support these investigations once it commences rather than triggering new investigations. The process of undertaking a financial investigation can take some time within the bank and to advance through the criminal justice system as it is required to go via the financial intelligence unit before arriving for law enforcement action. If there is potential wrongdoing, there are a few tools that banks can use. These are detailed below:

⇒ Obtain further Customer Due Diligence (CDD)[25] documentation and/or supporting documents from the client.
⇒ Block financial transactions linked to illicit financial and environmental crimes.

[25] Customer Due Diligence (CDD) is the process of gathering information on individuals and companies to verify their identity, their associations and other personal or company data to verify the background of the client when opening an account at a bank. It is also known as KYC – Know Your Customer.

⇒ Monitor the alleged or potential criminal bank accounts.
⇒ Open a new financial investigation into the client.
⇒ Report suspicious activity for further law enforcement action.[26]
⇒ Exit the client if the activity was not within the banks "risk tolerance".

The consequences of non-compliance
Banks have been fined significant amounts by financial regulators linked to AML failures. They have a duty to ensure that they are not facilitating criminal activity and hence can be fined or prosecuted if they are linked to moving money linked to illegal acts. Increasing allegations in the media linking banks to financing companies involved in deforestation can also be a reputational risk that can damage the bank's brand and thus its ability to do business. Therefore, banks have an interest in combatting environmental crime as a predicate crime to money laundering.

4.3 Third-party due diligence

Third party due diligence is conducted by banks primarily in the context of extending finance. There are several NGOs (Bank Track, Forest and Finance, Global Witness and Greenpeace among others) that publish data on who finances companies involved in environmental crimes including mass deforestation and fossil fuels. These organisations believe that banks are key enablers for environmental damage and destruction by financing *inter alia* fossil fuel businesses and agri-businesses linked to deforestation. These organisations put pressure on banks to review their risk management policies on who they do business with and ensure that proper due diligence is conducted. A recent case study linked to ANZ Bank shows how banks can be held liable if they do not conduct sufficient due diligence (Refer to Figure 10).

[26] STR – Suspicious Transaction Report also known as a SAR – Suspicious Activity Report

Figure 10: ANZ Case Study – Due Diligence Failures

Case Study: The importance of conducting due diligence before extending financing – Banks

It was reported in 2020 that ANZ Bank would compensate more than 1000 Cambodian families involved in a dispute with sugar company Phnom Penh Sugar Company after ANZ financed the sugar company in early 2010s. The Cambodian families were displaced from their land by the sugar company without proper process and compensation (i.e., a "land grab"). ANZ returned the profits from the loan to Cambodian families after a complaint was lodged under the OECD Guidelines for Multi-National Enterprises for responsible business conduct. With alleged human rights abuses undertaken by the sugar company, this case has provided a precedent linked to those financing companies that may be involved in human rights abuses and highlights the deficiencies in the due diligence processes of the bank. The company being financed was involved in the displacement of land and other human rights abuses.

Source: https://www.reuters.com/article/us-cambodia-landrights-anz-idUSKCN20L1D3
https://www.inclusivedevelopment.net/equator-banks/anz-payment-to-displaced-cambodian-families-brings-landmark-human-rights-case-to-a-close/?utm_source=rss&utm_medium=rss&utm_campaign=anz-payment-to-displaced-cambodian-families-brings-landmark-human-rights-case-to-a-close

Actions banks can take when financing companies potentially linked to environmental harm include:

⇒ Enhanced due diligence including proactive on-site visits including a review of company controls, interviews with personnel etc.
⇒ Putting conditions on loans and finance around environmental practices.
⇒ Evaluating policies on environmental and human rights issues.
⇒ Withdrawing funding to companies linked to environmental crimes.

Another recent case shows the Norwegian Sovereign Wealth fund divesting from four companies for *"contributing to serious environmental damage."* This shows a growing trend and awareness not to invest and fund companies involved in environmental damage and destruction.

Figure 11: Sovereign Wealth Funds – Acting on allegations of environmental damage

Case Study: Conducting due diligence on investments - Sovereign Wealth Funds

The Norwegian Pension Fund excluded four entities from their investment portfolio on 29 September 2021 with the following announcement: **"***The Executive Board has decided to exclude the companies China Traditional Chinese Medicine Holdings Co Ltd, Beijing Tong Ren Tang Chinese Medicine Co Ltd, Tong Ren Tang Technologies Co Ltd, and China Grand Pharmaceutical and Healthcare Holdings Ltd due to unacceptable risk that the companies contribute to serious environmental damage."*

Source: https://www.nbim.no/en/the-fund/responsible-investment/exclusion-of-companies/

Conclusions & Recommendations

List aggregators can play a key role in combatting environmental crime throughout the investigation and due diligence process. The current data collection processes have been heavily weighted toward offender data linked to the illegal wildlife trade, illegal logging, and selected trafficking of marine species which could be expanded into wider environmental offences including companies involved in deforestation, illegal mining, waste trafficking and pollution crimes. Why utilise list aggregators to combat nature crimes?

⇒ **Companies** can utilise list aggregators to leverage the data on environmental offenders when performing up-front due diligence linked to purchasing decisions across the supply chain or when extending finance or investing in third parties.

⇒ **Banks and financial institutions** can also play a key role in combatting environmental crime by conducting due diligence on clients it extends finance to, along with conducting investigations into entities that may be linked to environmental crime and reporting these entities for further law enforcement action.

⇒ The EIA Environmental **Media Monitoring Programme** could play an instrumental role in creating new data points on environmental offenders that are included in list aggregator platforms.

Final Recommendations

In conclusion, the following items are recommended to continue this work:

1. **Raise awareness on how banks, companies and governments an identify and locate data on** environmental crime offenders through list aggregators like Refinitiv and Lexis Nexis and other non-profit organisations and portals including the EIA lists.

2. **Raise awareness on how to report environmental crimes** - create awareness of the channels to report environmental crime i.e.: through the Crime-Stoppers International app or Wildleaks. Also consider raising awareness of information-sharing platforms and how information can be leveraged by governments and the private sector for better collaboration i.e.: Government-led forums and UFW taskforces for example.

3. **Document and publicise legal challenges** to sharing data on environmental offenders and how this can be resolved.

4. **Support additional resources and encourage new partnerships to support the EIA Environmental Crime Media Monitoring Programme**. EIA need additional funding and resources to build the capacity of the dedicated environmental crime watchlist. With more data inputs from NGO partners and more pathways to distribute data to list aggregators, awareness of environmental offending is likely to be amplified. In addition, the scope of the data has the potential to be broader in its environmental focus. Further partnerships with existing information-sharing platforms could also enhance the pooling of data for action by decision-makers.

5. **Understand the pre-deal due diligence processes** - Further work could be undertaken to research and understand what due diligence is conducted by companies and financiers including sovereign wealth funds, pension funds, commercial banks and asset managers prior to their purchasing, investment, or financing decisions. For example: if there is an allegation of illegal land clearing in Indonesia, do banks put conditions on the loans or exit the relationship? What is the current industry practice with respect to allegations of involvement in environmental crime? There may be potential for a new education portal to guide some of these decisions including due diligence for organisations that may be doing business with higher-risk entities.

6. **Conduct further work on the numerous watchlists and sanctions lists** that are inputs into list aggregator systems and evaluate how these can be leveraged to combat environmental crime.

Appendix 1: Sanctions, Denied Party and PEP Lists

TRACE basic searches from 100s of Denied Parties and Politically Exposed Persons lists. These lists include but are not limited to:
400+ Global Watch/Sanctions Lists, including:

- 77 non-US national-level regulatory lists
- 36 non-US national level law enforcement organization lists
- 65 US state and local level regulators
- 68 US state and local level law enforcement organization lists
- 45 US national-level regulatory lists
- 48 US national-level law enforcement organization lists
- 18 multilateral and regional regulatory lists
- 3 multilateral law enforcement organization lists
- 48 PEP-relevant lists

- Key Sanction Lists include, but are not limited to:
- Australia DFAT UNSC Sanctions List
- Australia Reserve Bank - Burma Sanctioned Entities
- Australia Reserve Bank - Iran Sanctioned Entities
- Australia Reserve Bank - North Korea Sanctioned Entities
- Australia Reserve Bank - Zimbabwe Sanctioned Entities
- Canada OSFI Cumulative Warning List
- Canada OSFI Entities List
- Canada OSFI Individuals List
- Canada OSFI UN Sanctions Act Resolution on Iran
- US Commerce Dept BIS Denied Entities List
- US Commerce Dept BIS Unverified Entity List
- US Commerce Dept. BIS Denied Persons
- US Dept. of State Chem/Bio Weapons Sanctioned Entities
- US Dept. of State Defense Trade Ctrls - Administratively Debarred Parties
- US Dept. of State Defense Trade Ctrls - Statutorily Debarred Parties
- US Dept. of State EO 12938 Nonproliferation Sanctioned Entities

- US Dept. of State EO 13382 Nonproliferation Sanctioned Entities
- US Dept. of State Foreign Terrorist Organizations
- US Dept. of State Iran & Syria Nonproliferation Sanctioned Entities
- US Dept. of State Iran Nonproliferation Act of 2000 Sanctions
- US Dept. of State Iran-Iraq Nonproliferation Act Sanctions List
- US Dept. of State Missile Sanctions Law Entities List
- US Dept. of State Missile Sanctions Law Entities List
- US Dept. of State Terrorist Exclusion List
- US Dept. of State Transfer of Lethal Military Equipment Sanctions
- EU Consolidated List of Sanctioned Persons, Groups, & Entities
- FBI Ten Most Wanted
- Interpol Most Wanted Fugitives
- Japan Finance Ministry Asset Freeze List

- US Treasury Dept. Designated Charities and Fronts for FTOs
- US Treasury Dept. FinCEN Advisory Notice List on Iran
- US Treasury Dept. FinCEN Section 311 Measures
- US Treasury Dept. OFAC Palestinian Legis. Council List
- US Treasury Dept. OFAC Specially Designated Nationals List
- UK HM Treasury Financial Sanctions Target List
- UK HM Treasury Investment Ban List
- UK Home Office/Ofc for Security & CT Proscribed Terror Groups
- UNSC Resolution 1132 Sierra Leone
- UNSC Resolution 1269 Al-Qa'ida and Taliban
- UNSC Resolution 1521 Liberia
- UNSC Resolution 1532 Liberia
- UNSC Resolution 1533 Congo
- UNSC Resolution 1533 Congo
- UNSC Resolution 1572 Cote D'Ivoire
- UNSC Resolution 1737 and 1747 Iran
- UNSC Resolution 1747 Iran


C4GA
THE CENTRE FOR GLOBAL ADVANCEMENT