# 反洗钱国际动态编译

（2021 年）总第 1 期

人民银行杭州中心支行反洗钱处　　2021 年 7 月 4 日

## 卷首语

为准确把握国际反洗钱前沿领域，增进浙江省内各单位间反洗钱信息合作交流，人民银行杭州中心支行反洗钱处结合前期编译工作情况，创立《反洗钱国际动态编译》刊物，面向全省各人民银行、义务机构不定期刊发。近期，我处组织省内平安银行、网商银行、江苏银行、浙商银行、中国银行等五家单位共同编译文献《A Reporter’s Guide: How to Investigate Organized Crime’s Finance（记者指南：如何调查有组织犯罪的金融状况）》，现将文献原文以及译文编发，供学习交流。希望各单位积极选派外语水平高、能力素质强的反洗钱专家参与支持我省反洗钱国际动态编译工作。

# A Reporter's Guide: How to Investigate Organized Crime's Finances
# 记者指南：如何调查有组织犯罪的金融状况

Editor's Note: For the next several weeks, GIJN is running a series drawn from our forthcoming Reporter's Guide to Investigating Organized Crime, which will debut in full in November at the Global Investigative Journalism Conference. This section, which focuses on money laundering, was written by Paul Radu, co-founder of the Organized Crime and Corruption Reporting Project. For those interested in more tips and tools on covering money laundering, OCCRP hosts a June 15 webinar, "Dirty Finance in Africa," followed by GIJN's own two-part "Investigating Company Finances" webinar, hosted by Finance Uncovered's Nick Mathiason on June 17 and June 23.

编者按:在接下来的几周里，全球调查新闻网将从我们即将出版的《调查有组织犯罪记者指南》(Reporter 's Guide to Investigative Organized Crime)中摘录一系列内容，并将于 11 月在全球调查新闻会议(Global Investigative Journalism Conference)上全面亮相。本节的重点是洗钱，由 Paul Radu 撰写，他是有组织犯罪和腐败报告项目的共同创始人。对于那些对更多关于洗钱的技巧和工具感兴趣的人，有组织犯罪和腐败报告项目（OCCRP）将于 6 月 15 日举办一个名为"非洲肮脏金融"的网络研讨会，随后全球调查新闻网将在 6 月 17 日和 23 日举办"调查公司财务"网络研讨会，由金融揭秘栏目的 Nick Mathiason 主持，该研讨会由两部分组成。

Most of the criminals I investigated over the past two decades could have been some of the world's best entrepreneurs. They had what it takes: resourcefulness, creativity, fast thinking, motivation, the ability to network and lead, and an obvious if uncanny attraction to risk. Many of them could have been on par with the Elon Musks of the legitimate business world, but they chose crime instead and their skill sets made them into some of the most dangerous and toxic people on the planet.

过去二十年里，我调查过的大多数罪犯本可以是世界上最优秀的企业家。他们具备成功所需的条件:足智多谋、创造力、思维敏捷、积极主动、人际交往能力和领导能力，以及对风险的明显吸引力。他们中的许多人本可以与合法商业世界中的埃隆·马斯克相提并论，但他们却选择了犯罪，他们的技能使他们成为这个星球上最危险、最有毒的人。

They think big and their business plans are simple: “more victims, more money.” And their life is made easier by the fact that most high-level criminals operate with impunity at a continental or even global scale, where they have no natural enemy because law enforcement is generally confined by national borders and national interests.

他们想得很多，他们的商业计划也很简单:“更多的受害者，更多的钱。”大多数高级犯罪分子在大陆甚至全球范围内活动而不受惩罚，这让他们的日子好过了很多，因为执法通常受到国家边界和国家利益的限制，他们在大陆甚至全球范围内没有敌人。

**Part One: How It Works**

**第一部分:如何工作**

Understanding how criminals structure their businesses and identifying the errors they make … is crucial when investigating high-level organized crime and corruption.

在调查有组织高级犯罪和腐败时，了解罪犯是如何组织其业务并识别他们所犯的错误……是至关重要的。

The Financial Blueprints of Crime

犯罪的金融蓝图

Because of the complications arising from transnational criminal enterprises, the fight against organized crime is mostly left to journalists and activists, who can network across borders and work in the public interest. But news organizations willing to take on one of the most powerful threats on the planet are limited in number and typically under resourced. The good news is investigative reporters have realized with the advent of cross-border collaborations that crime is, in many respects, a commodity and it follows general patterns making it easier to identify and expose. In short, if a criminal scheme works in a country or across a region, the same criminal model will be exported elsewhere in the world. It is the criminal blueprint and its elements that need to be understood to efficiently follow the money and stop criminals from doing business as usual.

由于跨国犯罪企业带来的复杂性，打击有组织犯罪的工作主要由记者和活动

家负责，他们可以跨国界建立网络，为公众利益而工作。但是，愿意应对地球上最强大威胁之一的新闻机构数量有限，而且通常资源不足。好消息是，随着跨国合作的出现，调查记者们已经意识到，犯罪在许多方面都是一种商品，它遵循一般模式，因此更容易被识别和揭露。 简而言之，如果一个犯罪计划在一个国家或一个地区有效，同样的犯罪模式将输出到世界其他地方。 因此需要了解犯罪蓝图及其要素，才能有效地追踪资金并阻止犯罪分子正常运营。

We have to understand our adversary to efficiently investigate and reveal its illegal activities. So, let’ s first go through some of the main instruments used by criminals to steal, hide, and invest their money. Then, in the second part, we’ll look at some of the best tools and ideas of our own to investigate and expose.

我们必须了解我们的对手，以便有效地调查和揭露他们的非法活动。那么，让我们先来看看罪犯用来偷窃、藏匿和投资的一些主要工具。然后，在第二部分中，我们将介绍一些我们自己用来调查和揭露的最好的工具和想法。

Criminals, both the ones just starting out as well as those who are already well established, have at their disposal regional and global infrastructure that is continuously built and maintained by what we at the Organized Crime and Corruption Reporting Project (OCCRP) call the“criminal services industry.”This infrastructure entails scores of lawyers, bankers, accountants, company formation agents, hackers, reputation management companies, and many others who make money by enabling the crime and by helping the criminals invest their ill-gotten money. So, what are the main elements of a crime on the money side?

无论是刚刚起步的还是已经成熟的犯罪分子，都可以使用区域和全球基础设施，这些基础设施由“有组织犯罪和腐败报告项目 ”(OCCRP)中所称的“犯罪服务产业”不断构建和维护。这种基础设施需要大量的律师、银行家、会计师、公司设立代理人、黑客、声誉管理公司以及许多其他通过支持和帮助犯罪分子投资来赚钱的的公司。 那么，金钱方面的犯罪的主要要素是什么？

Offshore-Type Companies

离岸型公司

A lot has been written about the offshore financial industry and the secretive companies that allow criminals to covertly steal and move large amounts of money

across jurisdictions. Projects such as Offshore Crime, Inc., Panama Papers, and others brought this illicit money-laundering industry into the spotlight, and subsequent large collaborations such as OCCRP’ s ongoing OpenLux project have highlighted that many landlocked countries such as Luxembourg provide or provided the same level of secrecy as the more traditional offshore locations. Understanding how criminals structure their businesses and identifying the errors they make or were forced to make is crucial when investigating high-level organized crime and corruption.

关于离岸金融业和犯罪分子在不同司法管辖区窃取和转移大量资金的秘密公司的报道已经很多了。离岸犯罪公司（Offshore Crime，Inc.）、巴拿马文件（Panama Papers）等项目使这一非法洗钱行业备受关注，随后的大型合作，如 OCCRP 正在进行的 OpenLux 项目，都强调了许多内陆国家，如卢森堡提供或提供了与更传统的离岸地点相同的保密级别。在调查高层有组织犯罪和腐败时，了解犯罪分子是如何组织他们的业务，并识别他们所犯或被迫犯的错误是至关重要的。

## Proxies
## 代理

Organized crime needs to hide behind other identities — proxies —so the offshore companies can provide the required secrecy for their transactions. During our investigative work at OCCRP, we’ve identified three main types of proxies: unaware, semi-aware, and fully complicit proxies.

有组织的犯罪需要隐藏在其他身份（代理）后面，以便离岸公司可以为其交易提供所需的保密。在 OCCRP 的调查工作中，我们确定了三种主要类型的代理：不知情代理、半知情代理和完全同谋的代理。

Unaware proxies are people whose identities have been stolen (sometimes via large-scale information theft from internet service providers) and who have no idea that their name is being used to form a company or set up a bank account. Semi-aware proxies lend their identity documents in return for small amounts of money, but without being aware of the true extent of the criminality of the businesses or transactions tied to their name. Complicit proxies, as the name implies, are fully cognizant of the criminal schemes that they are abetting and get a chunk of the profits. Knowing what type of proxy is involved in a criminal scheme can determine what

steps need to be taken by the investigative reporter trying to expose it.

不知情的代理人是身份被盗(有时是通过互联网服务提供商的大规模信息盗窃)并且不知道自己的名字被用来组建公司或开设银行账户的人。半知情的代理人借出他们的身份证件以换取少量金钱,但并不了解与其姓名相关的企业或交易的真实犯罪程度。同谋代理人,顾名思义,完全了解他们教唆的犯罪计划并从中获得一大笔利润。了解犯罪计划中涉及哪种类型的代理人,可以让试图揭露它们的调查记者们知道需要采取哪些步骤。

## Banks
## 银行

Despite the recent rise of innovative products in the financial sector, such as cryptocurrencies, banks remain a critical part of the world's financial systems. They are natural targets for organized crime groups, who seek to insert themselves and take advantage of the banking sector in various ways. As in the case of proxies, some banks are fully complicit, some are unaware, and some seem unprepared and perhaps unwilling to halt the criminal funds flowing through their accounts.

尽管最近金融领域创新产品的兴起,如加密货币,银行仍然是世界金融体系的重要组成部分。它们是有组织犯罪集团的自然目标,这些集团寻求融入并以各种方式利用银行业。就像代理人的情况一样,一些银行是完全同谋的,一些银行是不知情的,一些银行似乎没有准备也不愿意阻止通过他们账户的犯罪资金。

The banking system is made of a myriad of small, medium, and large banks and their subsidiaries. It is important to point out that small banks can only join the global financial system if they open up what are called corresponding bank accounts with larger banks, which ensure access to worldwide wire transfers. We've investigated many small and even medium-sized banks that were fully or partially owned and operated by criminals, but they still relied upon the largest banks in the world to send and receive vast amounts of dirty money. Smart criminals realized a long time ago that, much like law enforcement agencies are often tripped up by jurisdictional constraints, cooperation is also lacking between banks and that the financial compliance systems are geared towards identifying individual or small batches of suspicious transactions. The FinCENFiles made clear how banks can fail to identify high-volume money laundering. Criminals used this to their advantage by splitting

large volumes of money between numerous banks and bank accounts, so no one bank would have a clear picture of their massive, money laundering operations.

银行系统由无数的小型、中型和大型银行及其子公司组成。重要的是要指出，小型银行只有在大型银行开设了所谓相应的银行账户，才能加入全球金融体系，这确保了全球电汇的使用。我们调查了许多完全或部分归属于犯罪团伙或其经营的中小型银行，但是他们仍然依靠世界上最大的银行来收付大量的脏钱。聪明的犯罪团伙很久以前就意识到，就像执法机构经常被管辖权的限制阻绊一样，银行之间也缺乏合作，金融合规体系旨在识别个别或小批量可疑交易。FinCEN 档案清楚地说明了银行对大规模洗钱是无法识别的。犯罪分子利用这一点在许多银行和银行账户之间分配大量资金来发挥他们的优势，所以没有一家银行能清楚地了解他们大规模的洗钱活动。

Fake Contracts and Invoices

假合同和发票

To execute widespread money laundering schemes, criminals use forged paperwork, fake contracts, and invoices that are attached to the banking transaction as justification. These fictitious invoices certify on paper that a cargo of, say, personal computers was sold from offshore company A to offshore company B. But, in fact, no real trade has taken place, even as the money travels between bank accounts. This illicit practice is called trade-based money laundering and it might account for the biggest chunk of this type of financial crime worldwide. It’s obviously impossible for a banking compliance officer to check the contents of every shipping container associated with a financial transaction — and organized crime counts on that.

为了执行广泛的洗钱计划，犯罪分子使用伪造的文书、假合同和附带银行交易的发票作为正当理由。这些虚构的发票以书面形式证明货物，如个人电脑是从离岸公司 A 卖给离岸公司 B 的。但是，事实上，即使钱在银行账户之间流动，也没有发生真正的交易。这种非法行为被称为基于贸易的洗钱，它可能是全世界此类金融犯罪的最大一部分。对于银行合规官来说，显然不可能检查与金融交易相关的每个集装箱的内容 -- 有组织犯罪就认准了这一点。

In other instances, fake paperwork attached to banking transactions certifies fictitious loans and services with the same results.

在其他情况下，同样的，这些假文书附带的银行交易又为虚拟贷款和服务做

了认证。

The secret to efficient money laundering involves offering these four components as a full package to criminal groups and corrupt politicians. In fact, the criminal services industry even issues fraud manuals — sets of instructions on how to deploy companies, bank accounts, proxies, and fake invoices without triggering scrutiny from banking regulators or law enforcement. This is an example of what one of these money laundering manuals promoted by a bank in Latvia and uncovered by OCCRP - was advising clients to do:

有效洗钱的秘诀包括将这四个组成部分作为一个完整的打包方案，提供给犯罪集团和腐败的政治家。事实上，犯罪服务行业甚至发布欺诈手册 -- 一套关于如何在不触发银行监管机构或执法部门审查的情况下部署公司、银行账户、代理人和伪造发票的说明。以下是诸多洗钱手册中的其中一个例子，由一家拉脱维亚银行宣扬并被 OCCRP 披露-- 建议客户这样做：

“The delivery conditions specified in the contract or invoice should be realistic: When you specify goods, you have to think how they are going to be ‘shipped’ (weight of the cargo, volumes, address of the manufacturing plant, type of transport: road, rail, or ship.) In the case of ‘shipping’ of goods with very large volume or size, please specify a factory close to railroad or port.”

“合同或发票中规定的交货条件应该是现实的：当你指定货物时，你必须考虑它们将如何 “运输”（货物的重量、体积、制造工厂的地址，运输类型：公路、铁路或轮船。），在“运输” 非常大体积或尺寸的货物的情况下，请指定靠近铁路或港口的工厂。”

At OCCRP we call these turnkey money laundering systems “laundromats.” They act like all-purpose financial vehicles and are typically set up by a bank or other financial services company with the intent of helping clients launder the proceeds of crime, hide ownership of assets, embezzle funds from companies, evade taxes and currency restrictions, or move money offshore. OCCRP coined the term in 2014 with its investigation “The Russian Laundromat.”

在 OCCRP，我们称这些全包式洗钱系统为 “自助洗衣店”。它们就像通用的金融工具，通常由银行或其他金融服务公司设立，旨在帮助客户洗钱犯罪所得，隐藏资产所有权、挪用公司资金、逃税和货币限制，或者把钱转移到海外。OCCRP

在 2014 年通过调查 “俄罗斯自助洗衣店” 创造了这个词。

A laundromat is the financial-world equivalent of the TOR network browser, which provides users complete anonymity on the internet. Laundromats allow people to split laundered money among different banks so that, much like with TOR, secrecy is preserved because no single institution has a full picture of what is going on.

自助洗衣店相当于金融世界的 TOR 网络浏览器，它为用户在互联网上提供完全匿名的服务。自助洗衣店允许人们将洗过的钱分给不同的银行，这样就像 TOR 一样保密，因为没有一个机构能全面了解正在发生的事情。

Laundromats are made up of companies scattered across the world that appear independent but are actually controlled by a single party -usually the bank. The laundering process begins when a client wires money to a node in the network, often using fake paperwork showing a good or service being bought or sold. From there, the money’s parceled out to the other nodes, accompanied by more bogus paperwork. Eventually, the money is sent to an offshore company or other destination chosen by the client (minus a commission for the laundromat’s operators). The ownership and origin of the money is lost in the dizzying number of transactions, rendering it nearly untraceable, even by law enforcement. (For more on how this works, check out OCCRP’s laundromat FAQ.)

自助洗衣店是由分散在世界各地的公司组成，这些公司看起来是独立的，但实际上是由一个角色控制的 -- 通常是银行。当客户把钱汇到网络中的一个节点时，洗钱过程就开始了，通常使用伪造的文件来显示货物或服务被买卖。从那里，钱被分配到其他节点，伴随着更多虚假的文书工作。最终，这笔钱被送到离岸公司或客户选择的其他目的地（减去自助洗衣店运营商的佣金）。这笔钱的所有权和来源在令人眼花缭乱的交易数量中丢失，甚至执法部门也几乎无法追踪。（有关其工作原理的更多信息，请查看 OCCRP 的自助洗衣店常见问题解答。）

A clear example of how laundromats can evade scrutiny by some of the largest banks in the world was evident in a leaked, internal Deutsche Bank document, which details the bank’s failure to detect the Russian Laundromat that manipulated its global financial infrastructure.

在一份泄露的德意志银行内部文件中，一个明显的例子证明了自助洗衣店是如何逃避世界上一些最大银行的审查的，其中详细描述了该银行未能发现操纵其

全球金融基础设施的俄罗斯自助洗衣店。

There are many examples of how organized crime manipulates the financial systems of the world. Though the following are three examples from three different geographical regions, the pattern repeats itself and involves all or a smaller subset of the elements of the Russian Laundromat conspiracy above.

有组织犯罪如何操纵世界金融体系的例子有很多。尽管以下是来自三个不同地理区域的三个例子，但这种模式会重复出现，并涉及上述俄罗斯自助洗衣店阴谋的全部或一小部分。德意志银行泄露给 OCCRP 关于洗钱的内部备忘录，描述了该银行如何在不知情的情况下成为俄罗斯大规模洗钱计划的合作伙伴。

图片：截图


The Azerbaijani Laundromat and Iran’s Anti-sanction ‘Economic Jihad’

阿塞拜疆“自助洗衣店”事件与伊朗反制裁“经济圣战”

The Azerbaijani Laundromat primarily allowed the elites in Baku, Azerbaijan, to bribe European politicians and to siphon hundreds of millions out of the country. But OCCRP discovered that this money laundering machine was also used by Iran to bypass US and European sanctions thanks to the help of an organized crime group led by Reza Zarrab, an Iranian-Turkish criminal very close to the Turkish President Recep Tayyip Erdogan. The money laundering conducted by Zarrab had all the classic elements enumerated above and turned into a growing geopolitical scandal between Turkey, the US, and Iran — and shows how organized crime

thrives in times of unrest and can exploit political divisions.

阿塞拜疆“自助洗衣店”模式主要允许来自阿塞拜疆巴库的精英们贿赂欧洲政治家，并将数亿资金从阿塞拜疆带走。但有组织犯罪与腐败报道项目组(简称OCCRP)发现，这台洗钱机器也被伊朗用来绕过美国和欧洲的制裁，这要归功于伊朗-土耳其罪犯里扎·扎拉布(Reza Zarrab)领导的一个有组织犯罪，这位伊朗-土耳其罪犯里扎·扎拉布(Reza Zarrab)与土耳其总统雷杰普·塔伊普·埃尔多安(Recep Tayyip Erdogan)关系非常密切。里扎·扎拉布进行的洗钱活动具有上述所有经典要素，并演变成土耳其、美国和伊朗之间日益严重的地缘政治丑闻—这也表明有组织犯罪利用政治分歧，在动荡时期是何等猖獗。

The Troika Laundromat

三巨头“自助洗衣店”模式

The Troika Laundromat comprised a complex financial system that allowed Russian oligarchs and politicians in the highest echelons of power to secretly invest their ill-gotten millions, evade taxes, acquire shares in state-owned companies, buy real estate in Russia and abroad, and much more. The Troika Laundromat was designed to hide the people behind these transactions and was discovered by OCCRP and its partners through careful data analysis and thorough investigative work. The investigation involved one of the largest releases of banking information, some 1.3 million leaked transactions from 238,000 companies. To see a video explainer of the scheme, click here.

三巨头“自助洗衣店”模式( Troika Laundromat )由一个复杂的金融系统组成，它允许俄罗斯寡头和最高权力层的政客秘密投资不义之财、逃税、收购国有企业的股份，并在俄罗斯和海外购置房产等。经有组织犯罪与腐败报道项目组(简称OCCRP)及其合作伙伴仔细的数据分析和彻底的调查之后发现：三巨头“自助洗衣店”事件的目的是隐藏这些交易背后的人。此次调查揭露了一起最大规模的银行信息泄露事件，涉及 238000 家公司约 130 万笔交易。要看这个事件的视频解说请点击这里。

The Troika Laundromat exposé was born out of data work done on a large set of very dry banking transactions. We had to look for patterns in order to identify and isolate transactions that stemmed from what we later defined as the Troika Laundromat. We had to look for the errors, the bad links, in order to identify who

was the organizer and who were the users of the system. Through careful data analysis, we finally found out that the bankers putting this together made a small, but fatal, mistake: they consistently reused just three shell companies to make payments to formation agents in order to set up dozens of other offshore companies that were themselves involved in transacting billions of dollars. These payments, which were only in the hundreds of dollars each, were of course lost in a sea of millions of much larger transactions, so we had to find them and trace them back to recognize they were part of a larger pattern. The whole Troika Laundromat came in focus after identifying this common thread.

三巨头“自助洗衣店”该新闻调查是通过对大量且枯燥的银行交易数据进行分析才得出的。为了识别和隔离三巨头“自助洗衣店”相关交易，我们必须寻找其中的交易模式；为了确定谁是组织者和谁是系统用户，我们必须寻找其中的错误及恶意链接。经过仔细的数据分析，我们最终发现，三巨头“自助洗衣店”背后的庄家们把这些交易组合在一起时犯了一个小而致命的错误：他们为了建立起数十家离岸公司，以便操作自己数十亿美元交易，一直只利用三家空壳公司向这些离岸公司支付款项。而这些付款，每笔只有几百美元，自然而然在数以百万计的大交易中被淹没，所以我们必须找到它们，并追溯到它们，并确认它们是这个巨大的洗钱模式的一部分。整个三巨头“自助洗衣店”的洗钱模式在确认了这条共同线索之后就变得清晰起来了。

Riviera Maya Gang

里维埃拉·玛雅帮派组织

The Riviera Maya Gang (RMG) was a ruthless and violent cross-border organization, and this case offers a clear example of how organized crime scales up and into different businesses. The bandits in this case started small in Europe as skimmers — people who steal debit and credit card numbers by implanting illegal devices or software into ATMs. Crossing continents, they then partnered up with a Mexican bank and managed to install more than 100 ATMs on the Riviera Maya — the tourist area between Cancun and Tulum in southern Mexico — generating more than $200 million a year in criminal gains. The RMG used fake documents, fake identities, and proxies not just to build their business, but also to offer shelter to fugitives from justice while using the same infrastructure to smuggle people from Mexico into the United States.

里维埃拉·玛雅帮派(RMG)是一个残忍和暴力的跨境组织，这起案件提供了一个明显的案例：即有组织犯罪是如何扩大并进入到不同的企业中的。在这个案例中，匪徒们起初在欧洲是做 ATM 机分离器的—即通过将非法设备或软件植入自动取款机，盗取借记卡和信用卡号码。然后，他们与一家墨西哥银行合作，在里维埃拉玛雅(RivieraMaya)--墨西哥南部坎昆(Cancun)和塔姆(Tulum)之间的旅游区--安装了 100 多部自动取款机，每年可获得 2 亿美元以上的犯罪收益。里维埃拉·玛雅帮派组织（RMG）使用假文件、假身份和代理，不仅是为了建立他们的业务，而且也为了替逃犯提供司法庇护，该跨境组织同时利用同样的基础设施将墨西哥人偷运到美国。

**Part Two: How to Untangle It—Tips & Tools**

**第二部分：如何解密案件——提示与工具**

Investigative reporters should increase their focus on property records to untangle the investments and the scale of money laundering on the side of organized crime.

调查记者应更多地关注财产记录，以理清有组织犯罪方面的投资和洗钱规模。

As seen in the examples above, organized crime groups can be quite sophisticated when stealing, hiding, and investing their money. But one thing they cannot control is time. And with each passing day, journalists, activists, and other investigators are garnering more transnational reporting experience while governments around the world implement more rules about transparency, company ownership, and property.

从上面的例子中可以看出，有组织犯罪集团在窃取、隐藏和投资他们的钱时可能非常老练。但他们无法控制的一件事是时间。随着时间一天天过去，记者、活动家和其他调查人员正在积累更多跨国报道经验，而世界各国政府正在实施更多有关透明度、公司所有权和财产的规则。

Banking and Court Records

银行和法院记录

Access to bank records is the Holy Grail when investigating organized crime

financing, but banking records are difficult to obtain because they are confidential, private documents.

查阅银行记录对于调查有组织犯罪集团的财务状况就像“圣杯”一样有效，但银行记录很难获取，因为它是机密的私有资料。

Reporters can’t always count on leaks and whistleblowers inside of banks and financial regulators to hand over records.

调查人员不能总指望银行或金融监管机构的数据泄露或保密来获取数据。

But there is another way to get banking records. These types of documents are often attached to criminal court cases against organized crime or even to commercial, civil litigation.

但是还有另外一种途径可以获取银行记录。这类文件通常和法院案件信息联系在一起，包括有组织犯罪，或者商业、民事诉讼案件。

It all depends on the jurisdiction, and the US is a prolific source for global banking records that become public on the Public Access to Court Electronic Records (PACER) service.

这都取决于具体的司法管辖区，其中美国的国际银行记录信息丰富，这些银行记录被发布在公开法院电子记录（PACER）服务平台上。

For example, OCCRP obtained hundreds of thousands of banking records by checking PACER and filing freedom of information requests with US courts after that country opened a legal case against the Azerbaijani Laundromat kingpin, Reza Zarrab.

例如，在美国对阿塞拜疆自助洗衣店的主要负责人 Reza Zarrab 提起法律诉讼后，有组织犯罪和腐败报告项目（OCCRP）通过查阅公开法院电子记录（PACER）并向美国法院提交信息查询请求，获得了数十万条的银行记录。

Previously, we obtained similar records from courts in other parts of the world. These banking records are often subpoenaed in bulk by law enforcement agencies and are a boon for investigative reporters who can get hold of them.

显然，我们从世界其他地区的法院获得了类似的记录。这些银行记录被执法机构大量使用，这对于能够获得这些记录的调查记者来说是个福音。

Leaked suspicious activity reports (SAR) from financial institutions, like those obtained in the FinCEN Files investigation, can also offer a glimpse into the world of banking secrecy.

从金融机构公开的可疑活动报告（SAR)，例如从金融犯罪执法网络（FinCEN）调查文件中获得的报告，也可以让我们一窥银行机密。

Leaks will only grow in quality and quantity, and if used in conjunction with court records, they can be extremely valuable to investigative reporters and the public they serve.

泄漏的资料在质量和数量上会有所提升，如果这些与法庭记录结合使用，那对调查记者和公众来将会非常有价值。

Court records and especially commercial litigation between two criminal parties are also very useful to investigators as criminals get to launder their dirty clothes in public, as are divorce cases.

法院记录，尤其是两个犯罪主体之间的商业诉讼记录、离婚案件，对调查人员也非常有用，就像犯罪分子公开清洗他们的脏衣服引人注目。

Property Records

财产记录

Criminals like to own things and while the luxury car, watch, or other bling-y items are a must for many, the ill-gotten gains generated by organized crime often end up invested in real estates, like luxury mansions, or vast agricultural and forest lands. Investigative reporters should increase their focus on property records to untangle the investments and the scale of money laundering on the side of organized crime. In most countries, property documents are public records and will show the current owner, previous owners, as well as some financial details like the purchase price and taxes.

犯罪分子喜欢拥有财富，豪华汽车、手表或其他金闪闪的物品，对这些人来说是必需品，但有组织犯罪分子一般将他们获得的不义之财投资于房地产，如豪宅，广阔的农地和林地。调查记者应当提高对财产记录的关注，从罪犯的角度分析去解开投资和洗钱的谜团。 在大多数国家和地区，财产档案是公开资料，能找到当前所有者、先前所有者以及一些财务细节信息，例如购买价格和税款。

Company Records

公司记录

National and international registries of companies can provide information not only about shareholders and board members, but in many cases also contain a company’s financial data. On rare occasions, these records also reveal banking transactions, property records, and even granular information or beneficial ownership information about offshore-type companies that might be shareholders. Quite often we get information about a beneficial owner through registries of companies or property in places where these companies invest their illicit funds. Also, keep in mind that not all information is digitized and indexed in databases, so a trip or a phone call to the registry might give you access to a lot more data than what is available online.

国内和国际公司注册机构不仅可以提供有关股东和董事会成员的信息，而且在许多情况下还包含公司的财务数据。在极少数情况下，这些记录还会披露银行交易、财产记录，甚至可能包含作为股东的离岸公司的实际控制人的详细信息。我们常常能够通过犯罪分子利用不法资金进行投资时相关的公司或财产注册机构获得实际受益人的信息。需要注意的是，并非所有信息都已数据化并能通过数据库获取，因此通过电话咨询或直接前往登记处查询会比网上查询获取到更多的信息。

An important stage in exposing high-level money laundering is exposing the beneficial ownership of banks. Treat banks like any commercial company and try to find out who owns them. This is especially important in the case of newly formed, small- and medium-sized banks.

识别高级别的洗钱活动的一个重要阶段是揭露银行的实际所有人。 将银行当做商业企业并且找出最终的所有人。这对于新成立的中小型银行尤为重要。

Import-Export Databases

进出口数据库

Frequently, we use databases such as ImportGenius or Panjiva to track down import-export operations. These are expensive databases — downloading one year of a company’s US import data from ImportGenius costs $199 — but they can be

helpful to identify trade-based money laundering and the companies involved with it. We have used these databases to confirm if companies involved with the laundromats were also involved in other phony commercial operations. Of note: In many countries, the annual import-export transactions are available via national freedom-of-information laws, while the United Nations Comtrade site offers useful global trade data where import-export patterns can be identified.

我们经常使用 ImportGenius 或 Panjiva 等数据库来跟踪进出口贸易。这些都是昂贵的数据库——从 ImportGenius 下载一年一家公司的美国进口数据需要 199 美元——但它们有助于识别以贸易为基础的洗钱活动以及与之相关的公司。我们已经使用这些数据库来确认参与洗钱的公司是否也参与了其他虚假的商业活动。值得注意的是：在许多国家，每年的进出口交易数据都可以依据国家信息自由法合法获取，而联合国商品贸易网站提供了有用的全球贸易数据，可以确定进出口模式。

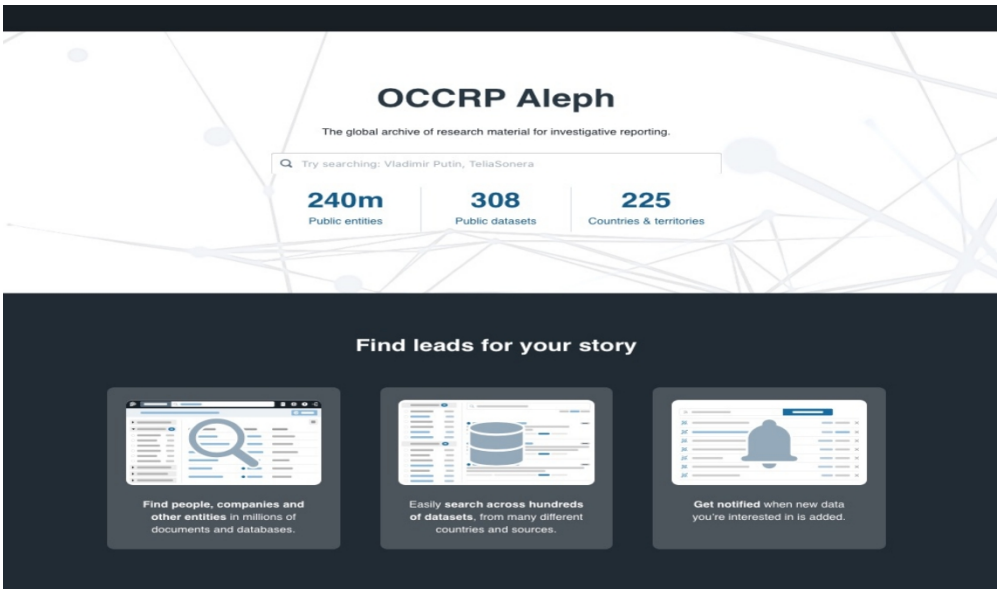
At OCCRP, we built a global archive of research material for investigative reporting called Aleph. Here, we index information on companies, property, bank accounts, court cases, leaks, and many other entities. But the indexing is just the beginning, as Aleph allows journalists to make sense of data and to identify the criminal patterns that are critical for starting a meaningful investigation in the public interest. Journalists can also keep person-of-interest watchlists inside Aleph and our system will continuously match the names in the lists against the other data contained within the system. This automates our workflow and helps ignite fresh and useful investigative reporting.

在 OCCRP（有组织犯罪和腐败报道项目），我们为调查性报道建立了一个全球性的研究资料档案库，名为 Aleph。在这里，我们索引了有关公司、财产、银行账户、法院案件、泄密和许多其他实体的信息。但索引只是一个开始，因为 Aleph 让记者能够理解数据，识别犯罪模式，这对于为公众利益展开有意义的调查至关重要。记者还可以在 Aleph 中保存感兴趣的人的观察名单，我们的系统将不断地将名单中的姓名与系统中包含的其他数据进行匹配。这自动化了我们的工作流程，并有助于激发出新鲜和有用的调查报告。

The OCCRP has developed Aleph, a useful resource that allows investigative journalists to search for public records and leaks. Image: Screenshot

OCCRP 开发了 Aleph，这是一种有用的资源，可以让调查记者搜索公共记录

和泄密信息。资料图：截图




**What Does the Future Hold?**

**未来会怎样？**

For the past few decades, transnational organized crime was many steps ahead of law enforcement, investigative reporters, and activists. Things started to change slowly with journalists joining forces across borders, but criminals still enjoy an advantage thanks to the huge resources at their disposal and because they are early adopters of new technology that allows them to stay one step ahead of law enforcement.

在过去的几十年里，跨国有组织犯罪比执法部门、调查记者和活动家领先了许多步。随着记者跨国联手，情况开始慢慢发生变化，但犯罪分子仍然享有优势，这要归功于他们掌握的巨大资源，也得益于他们是新技术的早期使用者，这使他们能够比执法部门领先一步。

One group often overlooked are so called criminal angel investors, people who finance other criminals because the return on investment is great and crime brings more opportunity to people used to this lifestyle. Investigative reporters need to better understand the financial ecosystem built around crime, where the criminal services industry thrives and develops new money laundering and covert investment techniques.

一个经常被忽视的群体是所谓的犯罪天使投资人，他们为其他犯罪分子提供

资金，因为投资回报率很高，犯罪给习惯这种生活方式的人带来了更多的机会。调查记者需要更好地了解围绕犯罪而建立的金融生态系统，犯罪服务业在这里蓬勃发展，并开发出新的洗钱和秘密投资技术。

To keep up with organized crime’s evolving techniques, investigative journalism organizations should invest time and money understanding cryptocurrencies, blockchain, non-fungible tokens (NFTs) and any other new tools of the trade criminals have adopted for their business models.

为了跟上有组织犯罪不断发展的技术，调查性新闻机构应投入时间和金钱，了解加密货币、区块链、不可替代代币（NFT）以及贸易犯罪分子在其商业模式中采用的任何其他新工具。

“Follow the money” will soon become “follow the code” (as in an algorithm), but in the end, it all takes a physical form in the shape of property and the visible lifestyle that crime brings with it.

“跟着钱走”很快就会变成“跟着代码走”（就像在一个算法中），但最终，它都会以财产的形式和犯罪带来的可见生活方式呈现出来。

Additional Resources

How to Follow the Money: Tips for Cross-border Investigations

A 10-Step Program to Fight Kleptocracy Around the World

GIJN Series: How to Uncover Corruption

额外资源

《如何跟踪资金：跨境调查的小贴士》

《打击全球犯罪统治的 10 步计划》

《GIJN 系列：如何揭露腐败》

Paul Radu is co-founder and chief of innovation at OCCRP. He founded the organization in 2007 with Drew Sullivan. He leads OCCRP’s major investigative projects, scopes regional expansion, and develops new strategies and technology to expose organized crime and corruption across borders.

paulradu 是 OCCRP 的联合创始人和创新主管。2007 年，他与德鲁·沙利文一起创立了这个组织。他领导 OCCRP 的主要调查项目，扩大区域范围，并开发新的战略和技术，以揭露跨国有组织犯罪和腐败。

**主送对象：**人民银行各市中心支行，杭州辖内各县（市）支行，各国有商业银行浙江省分行,浙商银行,省农信联社、交通银行浙江省分行,各股份制商业银行杭州分行,邮政储蓄银行浙江省分行,杭州银行,各城市商业银行杭州分行,各外资银行杭州分行,在杭各法人证券、保险、非银行支付机构，在杭各证券、保险机构浙江分公司。

**签　发：**叶天华　　**校　稿：**骆帅韬　　**电　话：**0571-87686471