



The OSINT Handbook for Anti-Financial Crime

How FIs can transform financial crime investigations with Open Source Intelligence



“Due to the rapid and continuing growth of publicly available and accessible data, we might very well say that what we now live in is the ‘Age of OSINT’.”

- Matthew Redhead
Senior Associate Fellow, RUSI



How can financial institutions adapt to this new age and make the most out of OSINT?

What's in this guide?

Financial crime is growing more complex and compliance requirements are tightening. Simply using superficial checks against curated databases mean that risk factors remain hidden.

Financial Institutions (FIs) need to use OSINT to stay ahead of criminals and regulations. Yet without knowledge of the right techniques and best practices, they won't see the full value of OSINT.



By the end of the guide, you'll understand how to harness OSINT efficiently to gain better insight into client and network risk.

Contents

What is OSINT?	...4
Why OSINT?	...5
Who's using OSINT?	...6
Where can FIs use OSINT?	...7
OSINT challenges	...9
OSINT technology	...11
Case study	...13
Next steps	...14

What is OSINT?

Open Source Intelligence (OSINT) allows organisations to leverage **publicly and commercially available information** to generate actionable insights. In an anti-financial crime context, this might mean using this information to get a more accurate picture of client or counterparty risk.

Much of this information exists online. But simply using a search engine to look up a subject of interest isn't OSINT. In fact, it's unlikely to uncover many new insights.

To understand why, let's have a look at the different collection techniques and sources available to OSINT investigators.

1

What do search engines surface?

Search engines don't rank results by relevance to your investigation. Instead, they're ordered by factors like SEO, search history and location. If you're using search engines without other investigative techniques, you're unlikely to find all the information you need.

2

How is the internet structured?

Under 7% of data on the internet exists on the surface web, the part of the internet indexed by search engines. Volume isn't everything, but this figure shows how much information you're missing if you're relying on traditional search engines.

3

Why use a range of sources?

OSINT investigators should make the most of the range of sources available to them. These include adverse news, PEPs and sanctions lists, corporate records, publicly available social media, and more.

When it's used properly, OSINT uncovers important context and insights that aren't evident through other sources of intelligence.

Why should FIs use OSINT?

With regulations tightening, fines growing and criminals becoming better at covering their tracks, it's clear that change is needed. FIs must move beyond simply ticking boxes when it comes to compliance.

Many organisations are moving towards an intelligence-led approach. OSINT is essential to this approach, as it allows FIs to generate more accurate intelligence to inform decisions. Let's have a look at some of the main reasons why FIs should be using OSINT:

Enable better risk-based decision-making



Simply relying on internal data and curated databases means missing important risk factors. FIs can get a fuller picture of client risk with OSINT, allowing them to make better-informed decisions and avoid being complicit in criminal activity.

Demonstrate commitment to stopping financial crime

OSINT can be transformative. Effective use demonstrates to regulators that an organisation is committed to countering financial crime.

Plus, some existing regulations recommended using OSINT – notably those surrounding Enhanced Due Diligence (EDD). By investing in OSINT now, organisations can future-proof their AFC processes.



Retain customer trust and protect the firm's reputation



Upholding a positive reputation is crucial to business success. OSINT allows FIs to safeguard against reputational and financial damage by avoiding regulatory transgressions.



Who's using OSINT?

With large growth in internet usage globally, there's much more open source information available than ever before. More and more organisations are recognising the value of OSINT in this internet-centric world.

High-profile cases led by organisations like Bellingcat have proven how much investigators can achieve using OSINT alone. So how can FIs make the most out of this growing form of intelligence?

Lots of FIs are already using OSINT – but they're not unlocking its full power

Adverse media checks are a form of OSINT, even if FIs aren't calling them that.

But adverse media is just one of the many types of open source data. FIs must learn to harness all the sources at their disposal to get a complete picture of risk.

Overcoming common misconceptions to see the true value of OSINT

Some pioneering FIs are already going beyond adverse media, striving to get a full view of their exposure to risk. However, OSINT remains undervalued in banks – common misconceptions place it as being unreliable, risky and difficult to use.

In reality, it's an extremely valuable source of intelligence that FIs can't afford to miss.

Where can FIs use OSINT?

It's clear that OSINT is a key asset in anti-financial crime investigations. FIs who aren't making the most of it are may be exposed to unnecessary hidden risk.

But where exactly should FIs be using OSINT? Let's recap some of the main use cases below.



Enhanced Due Diligence

EDD means building a deep understanding of a client so organisations can understand source of funds and get an accurate idea of associated risk.

Criminals may obscure their activity from official channels, making it crucial for FIs to review a range of sources to avoid facilitating criminal activity.



Key Sources: **corporate records** can reveal risky connections, whilst **local news** may offer insights not reported on in mainstream media.

Financial Intelligence

OSINT is uniquely suited to assist in building out networks and understanding connections. Proactively seeking out such intelligence is key to financial intelligence teams' success.



Key Sources: Combining **PEPs and sanctions watchlists, corporate records** and **publicly available social media allows** investigators to map networks and identify potential threats.

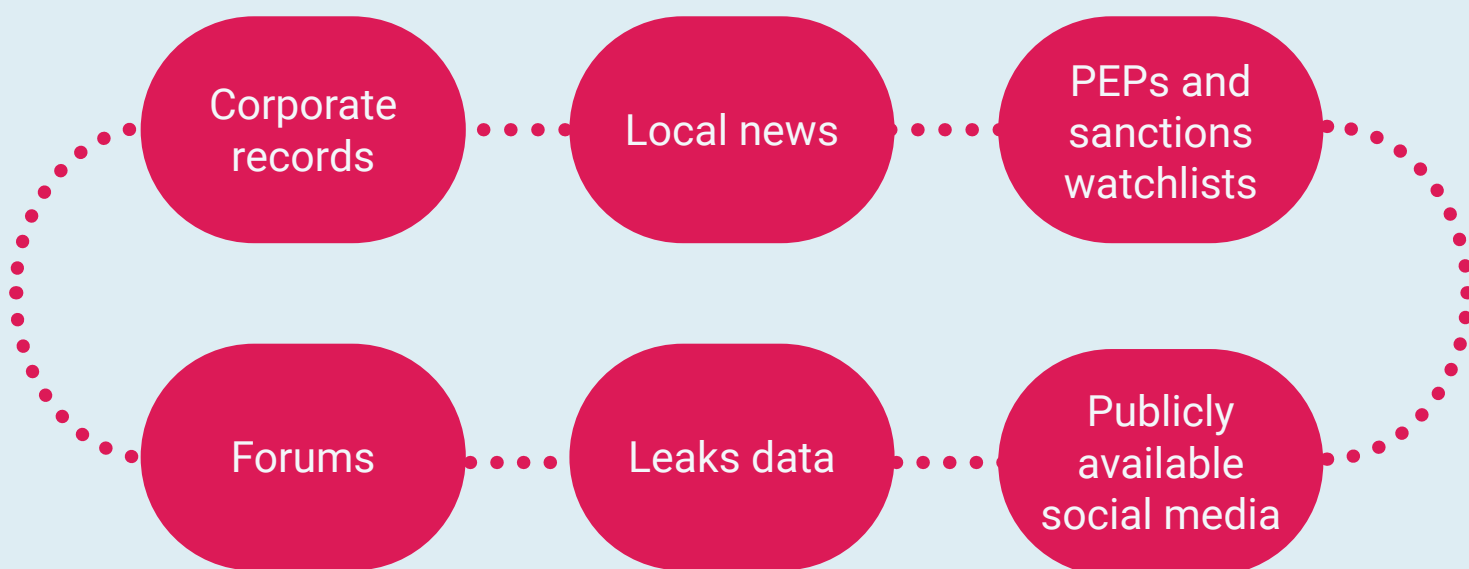
Where can FIs use OSINT?

Anti-Money Laundering

OSINT provides additional context when investigating beneficial ownership or suspicious connections, so firms can make better risk-based decisions.

.....

Key Sources: Supplementing **corporate records data** with information from **local news**, **forums**, or **publicly available social media** can help investigators understand obscured beneficial ownership.



Sanctions

Beneficial ownership rules are changing and sanctions evasion is growing more complex. Consulting sanctions lists isn't enough to guarantee compliance anymore. Combining official lists with OSINT means FIs can gather the full context behind transactions and client connections.

.....

Key sources: **Sanctions databases**, **leaks data** and **corporate records** can all reveal undeclared exposure to sanctions.

OSINT challenges

Whilst OSINT is a valuable resource, it can also be difficult to leverage. Below, we look at some of the common challenges anti-financial crime investigators might encounter when using OSINT.



Disparate sources and platforms

Accessing a range of sources manually can mean a lot of time is spent switching between platforms. This is very time-consuming and means it's easy to lose something important.

Yet, using just one source isn't an appropriate solution. We'll cover the best way to overcome this problem later in the guide.



Growing volumes of data

With the internet growing every day, there are huge volumes of data available to OSINT investigators. This can be challenging to navigate, and if you're operating manually it's hard to guarantee you've reviewed all the relevant data.

This challenge can seem insurmountable, but it's easy to overcome with the right training and technology.



Security concerns

When browsing open sources, it's crucial to anonymise your activity and ensure you're not exposing your organisation to additional risk. The burden to do this usually falls on the investigator, which takes up valuable time.

Some FIs might prefer to not use OSINT so they can bypass these concerns – but in doing so, they're opening themselves up to greater risk later on.

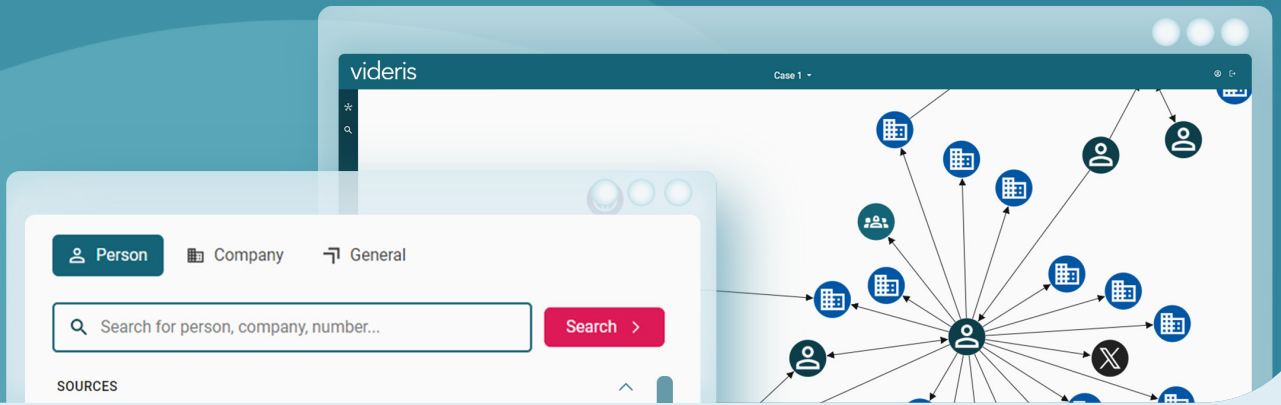


FIs often require cases to be completed in short timeframes so they can provide a smooth service for clients. As such, efficiency is a major concern.

Many of the OSINT challenges discussed above involve a lack of efficiency – but in the next section, we'll discuss how to overcome these difficulties and adapt OSINT processes so they're suited to the unique needs of FIs.



See how to overcome these challenges.



Overcoming OSINT challenges with targeted technology

Training on best practices paired with innovative technology can help FIs overcome OSINT challenges and get a fuller picture of risk.

However, it's important to note that not all OSINT tools are appropriate for FIs. Because OSINT is such a broad category, many OSINT tools are not adapted to the unique needs of FIs. With that in mind, here are some things to look for when picking technology to support your organisation's use of OSINT:



It's well suited to FIs: FIs have unique needs, with specific efficiency and security requirements. Find a vendor who understands this and has the expertise to meet these requirements.



It solves your main challenges: Different firms will have different challenges. Identify the problems that are most important for your organisation to solve before looking for a tool.



Excellent customer support is available: Every FI has unique requirements and challenges. Individualised customer support experienced in working with FIs allows you to ensure the tool meets your needs.



It's intuitive and easy-to-use: Your organisation will see value from the investment faster if it's easy to use. Plus, this means it can be expanded into further teams with less friction.



It's scalable: As your team and firm grows, will the technology you use be able to grow with it? A scalable tool means you can future-proof your investigations.



A single platform: Ideally, you should have one central OSINT platform with all the sources and features you need. This allows firms to streamline processes.

At Blackdot, we work closely with FIs to help them unlock the power of OSINT. Our OSINT platform, Videris, is designed to help investigators identify and prevent financial crime, and allows investigators to work up to 400% faster. **Get in touch today to see how it could help your organisation.**

blackdotsolutions.com/book-a-demo

Case Study

See how Videris supports Danske Bank's Financial Crime Compliance programme

The Challenge



Previously, OSINT was performed by investigators running manual Google searches. This approach limited access to data and produced inconsistent results, affecting the organisation's ability to identify all potential client risk.

The Solution

Danske Bank partnered with Blackdot, implementing Videris to enhance their OSINT capabilities.

Videris is a holistic OSINT solution, bringing together all the sources investigators need. It allows them to search, analyse and visualise this data from a single platform.

The Benefits

-  Improved identification of risk
-  Single, streamlined platform
-  Increased efficiency and effectiveness

“Videris has supported strengthening of our Financial Crime investigation function by providing us with more enhanced OSINT capabilities that enable our investigators to identify risks faster.”

Marjo Pikkukangas, Group Head of Suspicious Activity Reporting



Ready to start using
OSINT to uncover
hidden risk factors?



Get in touch
with us today.

blackdotsolutions.com/book-a-demo