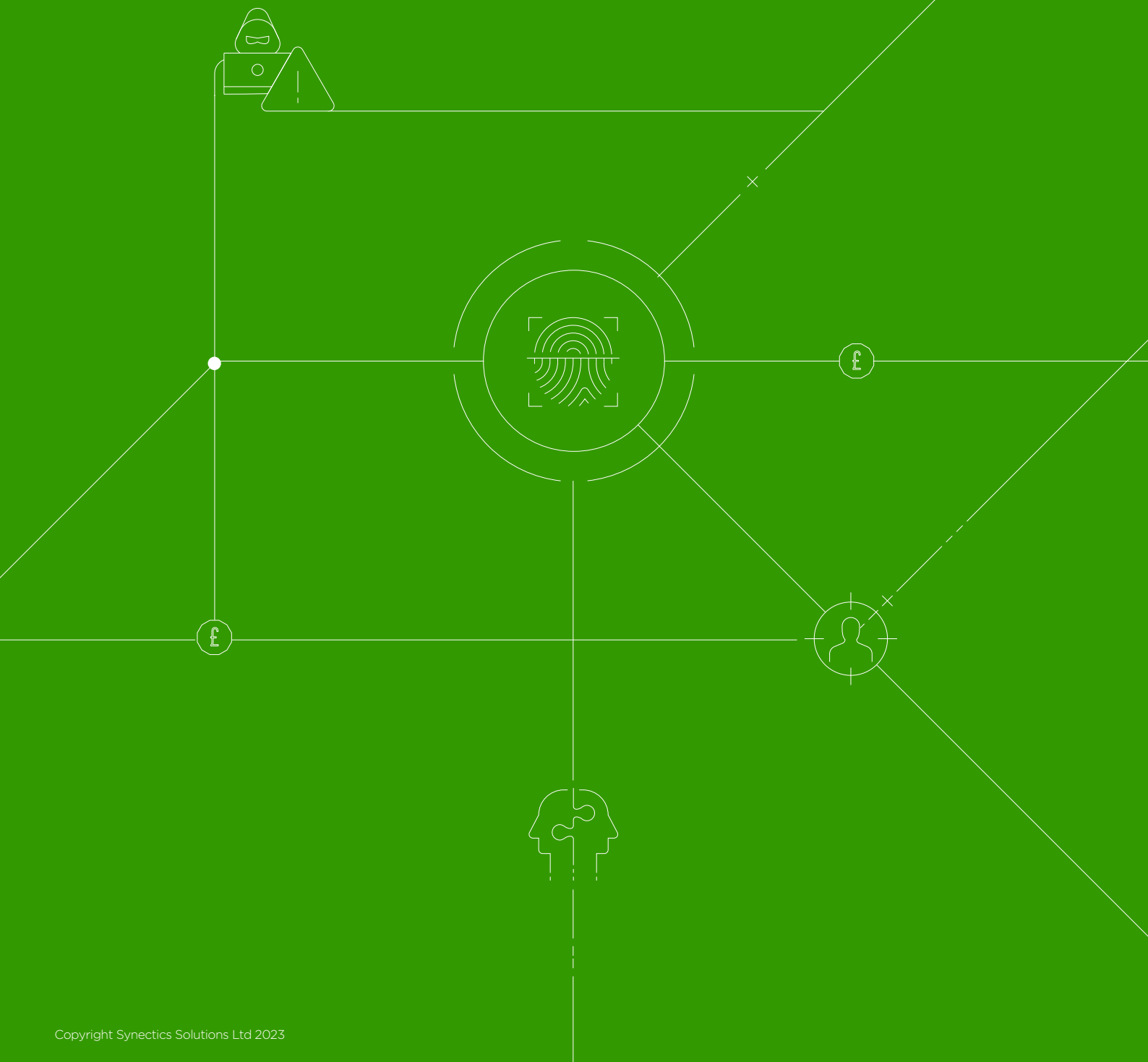
SYNECTICS SOLUTIONS

Economic Crime and Corporate Transparency Bill

Free to talk: what banks need to know about upcoming legislative provisions for sharing financial crime data

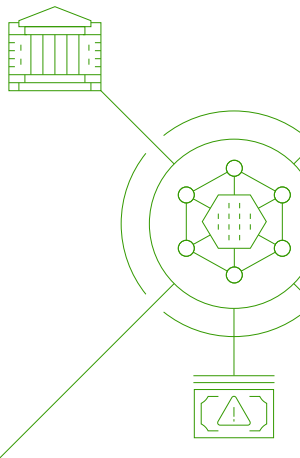


In 2020, the Intelligence and Security Select Committee produced a report on Russia which labelled London a 'laundromat' for corrupt money. A memorable label reflective of a much broader issue. The impact of financial crime on our society.

Despite having one of the toughest regulatory eco-systems for combatting money laundering and wider financial crime - the annual cost of such activities to the UK economy is estimated to be around **£37 billion.**

But things could be about to improve. Subtle but highly significant developments in the latest iteration of the **Economic Crime & Corporate Transparency Bill,** are poised to change the way banks and other regulated financial institutions communicate when it comes to suspicious customer activity.

Read on to learn about what's changed, what this means for peer-to-peer financial crime data sharing, and why this is good news in the fight against financial crime. **It's time to talk.**

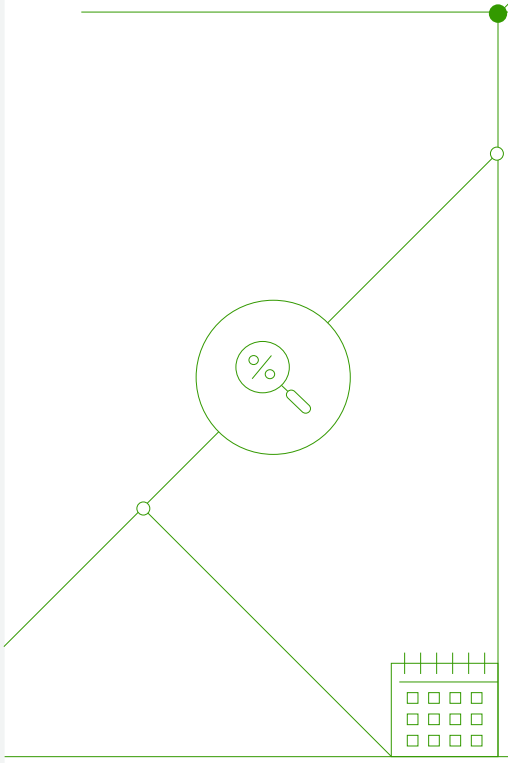


WHAT'S GONE SO WRONG?

With evidence suggesting such significant levels of money laundering in the UK, something is clearly going wrong. **But what exactly?**

Counter-intuitively, many in the industry have long argued that while our tough regulatory backdrop is essential in tackling financial crime, it's also partly to blame for specific failings. More precisely, that data privacy compliance requirements end up effectively gagging financial institutions from talking with each other (and with law enforcement agencies) more openly about legitimate suspicions of criminal activity.

Which is precisely why developments in the Economic Crime & Corporate Transparency Bill around data sharing are potentially game-changing. Before we go into these in more detail however, it's first useful to understand the traditional challenges institutions face when it comes to sharing intelligence on suspected financial crime.



Defining financial crime

According to the Government's Economic Crime Plan, financial or economic crime "refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others."

- **Does this cover fraud?** Yes.
- **Does this cover money laundering?** Yes.
- **Are the two the same when it comes to how banks and other financial service providers can report their suspicions?** No. And that's been the nub of a very contentious area for many years.

Practicalities of privacy: the fraud vs AML distinction

In the UK, banks can - and do - share vast volumes of fraud data with each other via fraud detection and risk mitigation platforms, examples of which include National SIRA, CIFAS, NFI etc. National SIRA alone has helped members save over £1billion in the last 12 months by enabling them to cross-refence financial product/service applications with the adverse information held.

They can also share real time fraud signals to warn each other of potential fraud perpetrators. Indeed, having a mechanism in place to this effect is a stipulated requirement for those wishing to be part of the UK Digital Identity and Attribute's Trust Framework.

In both cases, sharing such data is effectively compliant with GDPR requirements by way of a notable exemption from it; the exemption being that sharing fraud data is classed as being in the public's legitimate best interests.

There is, however, no such consensus established when it comes to sharing Anti Money Laundering (AML) concerns. And in the absence of any proactively enabling legislation (until now) to support economic crime related data sharing, this has left financial institutions severely restricted. Unable to talk to each other for falk to each other for fear of being in breach of privacy legislation and/or 'tipping off' suspects.

What is 'Tipping Off'

It is an offence to reveal information which could 'tip off' the subject of money laundering investigation and therefore potentially prejudice a law enforcement investigation into suspicious activity

Specifically, where that information came to be known in the course of business in the regulated sector.

A clear mandate to collaborate

This is about to change. Two particularly important provisions included in Part 5[1] of the Economic Crime mean that banks and other financial institutions will soon be able to:

Engage in bi-lateral messaging queries relevant to economic crime concerns, disapplying the duty of confidence in those instances; and

Share adverse information relating to economic crime such that this is accessible to deposit-taking, payment and virtual asset providers – the principal use-case for this envisaged as being the sharing of 'exit decision' information.

Specific criteria for bi-lateral messaging will have to be further defined, but in the future, banks will be able to share more customer data than they are currently able to in real time where they hold legitimate suspicion that a crime is taking place (see Scenario 1). And able to share information - most likely via platforms akin to current fraud databases - of individuals and/or businesses they have declined/exited where that decision is linked to suspicions of involvement in criminal activity (see Scenario 2). This also applies to sharing details, where appropriate, with law enforcement agencies.

1. Correct at time of publication

Scenario 1

1. A transaction is made between two accounts operated by different banks (Bank A & Bank B). The transaction triggers an alert in Bank B's TMS.

2. Bank B contacts Bank A via a secure connection, such as what is currently used by fraud database users. Bank A is offered the chance to collaborate on an investigation into the transaction.

3. Following the decision to collaborate, a joint investigation takes place into the transaction. Requisite KYC information for both customer accounts is combined into a joint case, to provide a broader view of the overall risk posed by the transaction.

4. Both banks have more information to hand to drive their subsequent decisioning process on this transaction. If crime is suspected, this could include exiting either customer dependent on the bank's risk appetite.

Scenario 2

1. Following the adjacent process in Scenario A, Bank A has chosen to exit their customer for money laundering.

2. Bank A share this data voluntarily via a data sharing syndicate, such as National SIRA.

3. Other National SIRA members are now able to use this exit information regarding the customer to affect future on-boarding decisions. Other organisations that have an existing relationship with this customer could be alerted via a perpetual KYC tool that the customer has been exited for money laundering.

In its Economic Crime Plan, the government stated that "No one agency or organisation has the information, intelligence or data necessary to combat economic crime alone. This can only be achieved by agencies and organisations having the appropriate powers, gateways, frameworks and culture in place to facilitate the effective, appropriate and targeted sharing and use of information".

These developments are an important step towards that envisaged future.

2. As at September 2021.

Will sharing financial crime data WORK?

EVERY INDICATION IS THAT IT WILL.

Last year, we supported research conducted by the FFIS programme (a partnership within the RUSI Centre for Financial Crime & Security Studies)

Lessons in private-private financial information sharing to detect and disrupt crime.

The paper, presented to policy makers and interested stakeholders, examined international developments in forms of information sharing between private sector entities to detect economic crime risk, covering both fraud prevention and AML domains of economic crime.

Of the 15 platforms/initiative analysed, 11 featured AML data sharing (alongside fraud data) with 4 being wholly AML focussed. The findings revealed that use of data-sharing platforms typically results in:

- **Improved detection rates of financial crime and greater discovery of subjects of interest;**
- **Faster speed of response;**
- **A reduction in the propensity for criminals to target participating institutions;**
- **In some cases, greater recovery of funds;**
- **A reduction in duplication of processes and cost due to pooled resources and shared value; and**
- **A reduction in risk displacement (for members)**

Doing more with data:

MOVING TOWARDS PREVENTION

Giving banks and other financial institutions greater ability to share AML and financial crime alerts immediately means the parties concerned are able to build more detailed risk profiles of their customers – the 'full picture' is no longer restricted to information gathered by in-house investigative teams.

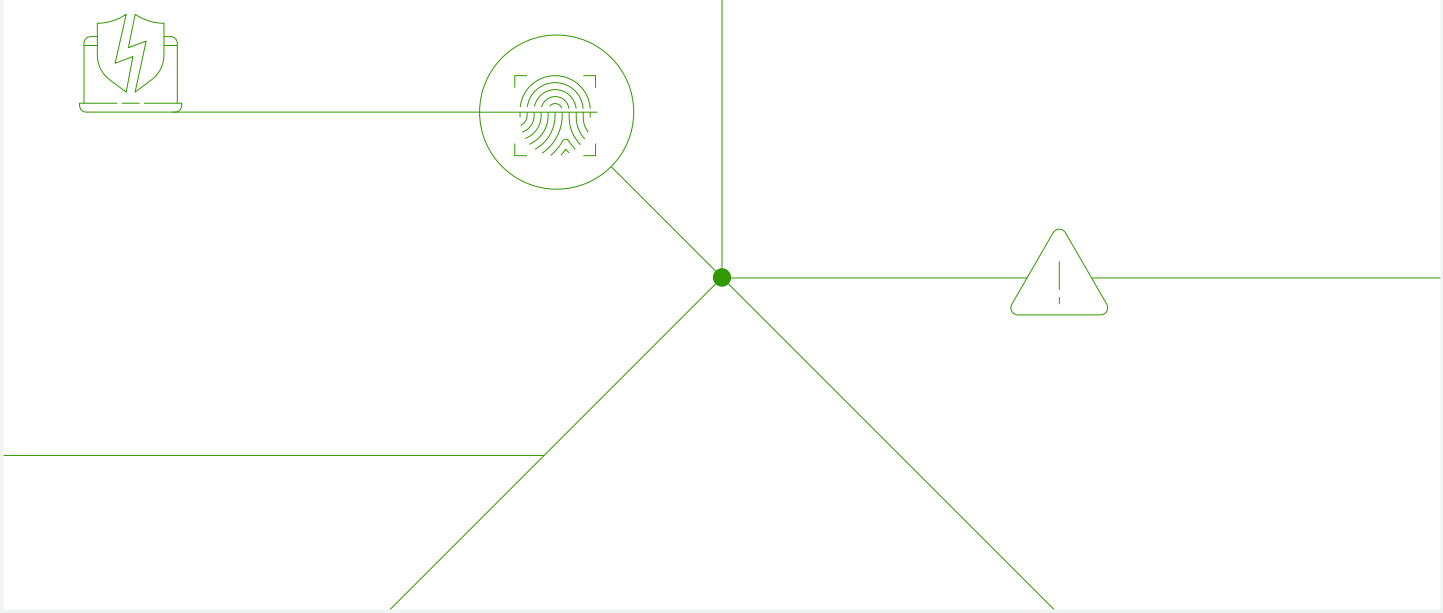
Given that financial crime is often typified by networks that span different accounts and banking organisations, this is hugely beneficial.

As well as improving detection rates of financial crime, this change in legislation also has significant implications for the prevention of money laundering and other financial crime.

The collation of exit data, for example, especially if also merged with existing adverse fraud data – a scenario we certainly envisage with National SIRA - will facilitate the creation of rich pools of information ideally suited for the application of machine learning and AI algorithms. Algorithms designed to identify anomalies and emerging modus operandi, which in turn facilitates the creation of proactive alerts that can warn banks and financial organisations if specific criteria are detected.

As identified in the Lessons in private-private financial information sharing to detect and disrupt crime research, "the potential to discover and refine typologies of suspicion" is significant. This includes having clear definitions of economic crime typologies, that are homogenous between participants in data sharing schemes and continuously evolve as the threat landscape changes.

Clear definitions for economic crime will further improve the efficacy of other models such as AI and predictive analytics. For example, the use of these techniques on shared fraud data is already generating significant savings for the industry. Appropriate and proportionate use of these techniques, in line with evolving and important regulations specific to this area, combined with consistent definitions to maximise the efficiency of the models, could be leveraged across economic crime use cases such as the detection of money laundering, or the triage of investigations following the generation of alerts from other systems such as a transaction monitoring system.



Example case: current account launch

Using the National SIRA database we trained our Precision predictive analytics solution to understand what good, bad, and suspicious looked like for one bank looking to offer a new type of current account. The system was set up to automatically route fraudulent applications to the correct teams. In just 12 months, the top scoring 15% identified by Precision accounted for 70% of fraudulent applications.

Unfounded suspicions: the need to share data responsibly

An understandable concern in relation to these developments is to question any exposure/risk involved in sharing data AML/financial crime data. Just because something is permitted doesn't mean there aren't still factors that require close consideration.

Strict governance models for managing data will be required, spanning both ethical and practical (e.g. cyber security, data transparency) concerns. A fact which lends weight to leveraging established fraud platforms – extending their scope to harness existing expertise and governance frameworks – rather than 'starting from scratch'.

On the subject of ethics, a significant area to address is that of 'unfounded suspicion. What happens if a bank flags the activity of a business or individual as concerning – indeed, reveals that they have exited a customer on this basis – where the party in question is in fact innocent of any financial crime?

As mentioned earlier, there will have to be further criteria developed in order to help prevent this scenario, i.e. to ensure suspicions shared reach a minimum threshold. But the eventuality cannot be ruled out entirely.

What can be ruled out are scenarios where individuals/businesses get refused access to financial services wholly on the basis of information shared. Indeed, many reciprocal sharing agreements in operation around the world have this as a stipulation.

With the right processes and obligations in place, for instance, a right to be informed and avenues to appeal for the customer, and an alert system which flags the need for additional investigations where initial evidence thresholds are not met, it is certainly possible to mitigate risk of unnecessary exclusion.

What's next and how we can help?

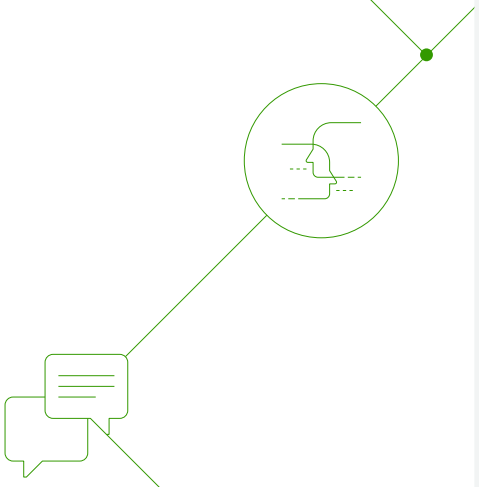
Synectics has been providing point solutions for wider economic crime for many years, and with fraud being a predicate crime to money laundering, we already highlight clear crossover between ecosystems.

For instance, designations in National SIRA such as "misuse of facility" encompass scenarios such as accounts being used to process illicit or disputed funds indicative of attempted money laundering.

We also process economic crime exit decisions for multiple financial institutions without sharing those decisions via National SIRA and can see the value in creating a separate but integrated model. One which builds on the information sharing framework National SIRA provides from a technological, operational, regulatory, and legal perspective. And which also leverages the reciprocity arrangement in place to both incentivise data sharing, and provide the mechanism for processing the collaboration needed.

There are hurdles to overcome. Consortium data sharing is only as strong as the organisations willingness to share, and with the upcoming bill focusing on voluntary sharing in the first instance, a clear business case needs to be developed for multiple institutions in order to get any consortium of this type off the ground.

Uniquely experienced in this process, and with a ready-made consortium to build upon in the shape of National SIRA, we are certainly ready to help.



TALK TO US TODAY

Tel: **+44 (0) 333 234 3409**

Email: **info@synectics-solutions.com**