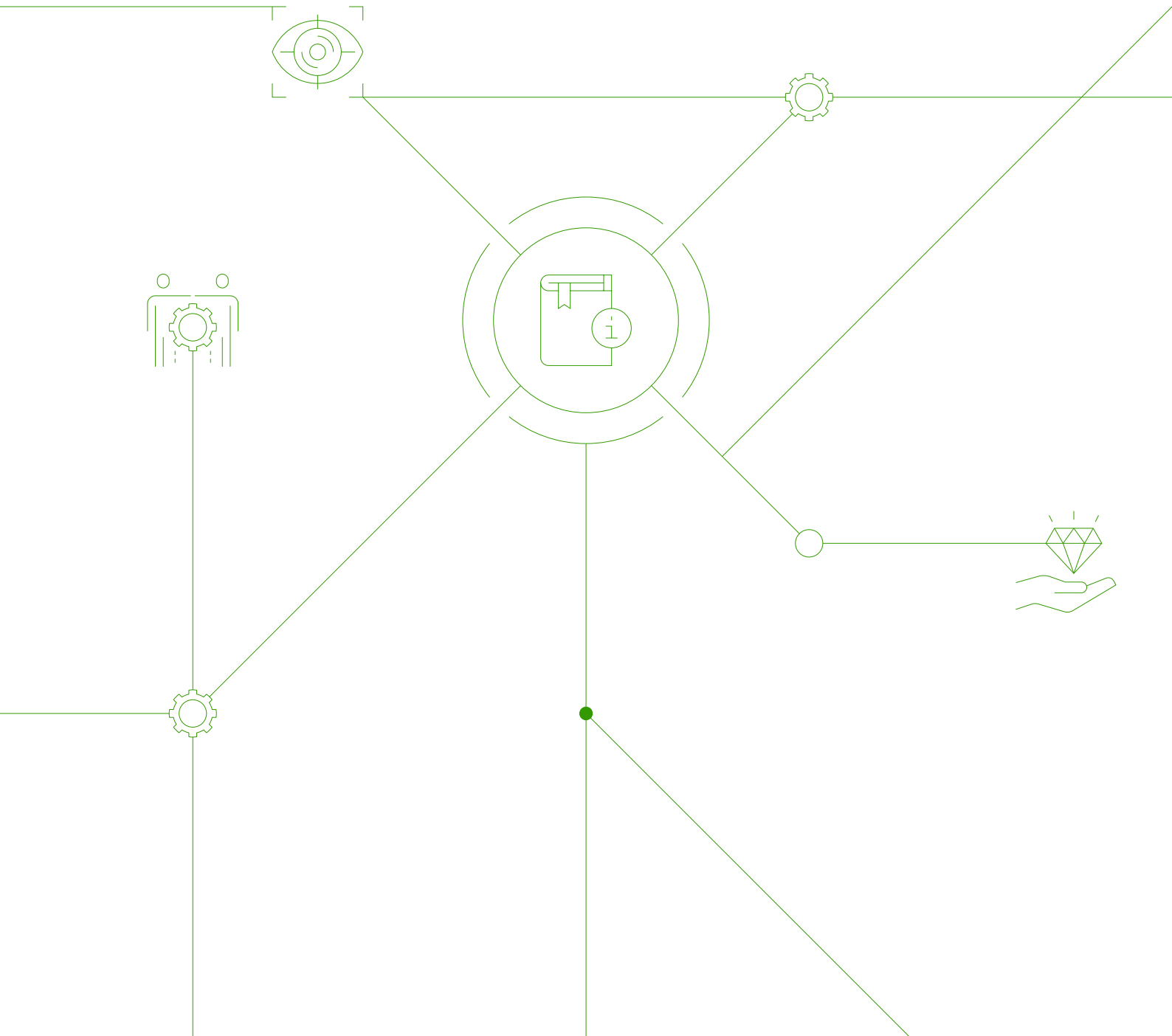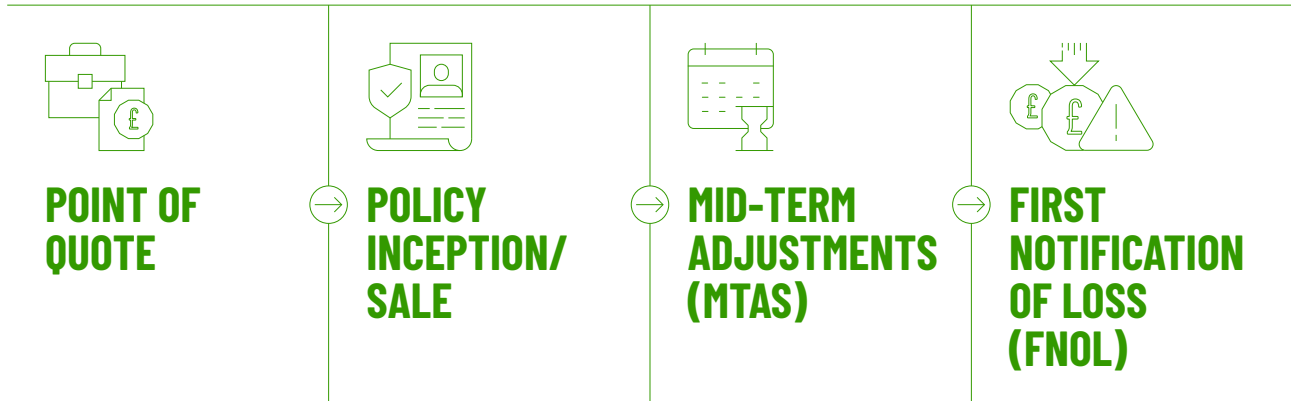# ENSURING BEST VALUE FROM NATIONAL SIRA

Detecting Insurance Fraud Via Data –
A Best Practice Guide

We all accept that the opportunity to commit fraud exists at every stage of the customer journey.

POINT OF QUOTE → **POLICY INCEPTION/ SALE** → **MID-TERM ADJUSTMENTS (MTAS)** → **FIRST NOTIFICATION OF LOSS (FNOL)**

→ **AND THROUGHOUT THE LIFECYCLE OF A CLAIM UP TO AND INCLUDING, THE POINT OF SETTLEMENT**

The good news is that this also means that there are just as many opportunities to identify and prevent this type of activity.

You're already working to disrupt fraud and wider financial crime and this guide will help ensure that you continue to get the most out of your National SIRA membership.

Data is king...

There's more data being captured today than at any point since the beginning of modern insurance in the 17th century.

This availability of – and thirst to interrogate – data is responsible for the plethora of Insurtechs and IT service providers coming to the market over the last decade. Each has something to offer.

All have valid solutions to specific industry problems including: fraud, pricing, actuarial analytics, claims workflow automation and unstructured data – the list goes on.

Quite simply, the number of tools available isn't a problem, more often than not it's the ability to access the data and siloed data sources that are.
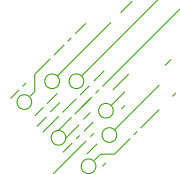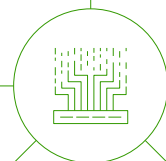
So how do you deal with siloed data?

In our experience organisations tend to do one of three things. Ignore the problem (intentionally or otherwise), migrate to a single new solution or outsource everything to a third party. Each solution has its merits.

1 — AVOID THE ISSUE	**2 — MIGRATE EVERYTHING TO A NEW, SINGLE IN-HOUSE SYSTEM**	**3 — SEND DATA FROM EACH LEGACY SYSTEM TO A CENTRALISED THIRD-PARTY SOLUTION AND USE THAT TO UNDERTAKE THE DESIRED ANALYTICS**
A very short-term solution that can undermine future development initiatives well beyond fraud and financial crime requirements.	Probably the preferred option for most organisations, but it's also the most expensive and, arguably, the slowest/hardest to implement. When it comes to fraud identification, many still require the use of an in-house and/or third-party solution (usually a combination of both) to plug any gaps.	This is usually the quickest route to goal but doesn't overcome many of the pain points of dealing with legacy/siloed systems, especially where APIs are not an option. High on that list is the double keying element that comes with keeping all systems in sync with one another.

Data, data, everywhere – now what do I do?

With data capture available at every stage of the customer journey, knowing what to do with it can be overwhelming.

The key is to Think Big Picture.

Analysing incoming data against your own historical records and experience is reactive – you will learn more about what you already know.

Add even more data? Surely not!

To obtain new intelligence and get the widest view of potential risk, you need to enrich your existing data by calling out to a variety of external data services, and/or pulling data from other internal silos.

Using the 'right' data at the right time will greatly improve the customer journey for the 99% of good, genuine customers. Not all data sources are equal, there are hundreds of different databases available from UK Government to industry specific to niche offerings from private enterprises and everything in between.

Some are enormous in terms of record volumes but if you're trying to force that dataset to do something that was never its intended use case, then you're likely to end up disappointed…or with a disappointed customer and that's worse still.
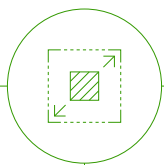
Start at the beginning

How do you know just what fraud risk a person presents if you've never seen them before?

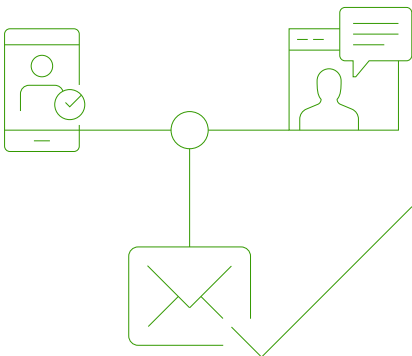Customer expectations are very different from those of ten, even five, years ago.

Insurers now need to do

more analytics in less time

and often with less information in order to offer competitive rates

This is hard enough in itself without trying to 'guess' if this new customer is intending to defraud you in the future.

Identifying previous links to fraud at Point of Quote (POQ) via National SIRA is your simplest first line of defence, before you take on a risk.

In less than half a second you can see if this potential new customer has had a history of committing fraud in the insurance or finance sectors.

Even if the person is 'clear', you can check if the address, telephone number or email address have been linked to previous fraud activity.

Armed with this fraud risk insight, insurers can price according to their risk appetite and redirect potential customers to different product offerings without that customer ever even being aware of the decisioning process taking place.

Welcome aboard

So, your new customer has accepted the quote, paid the premium and received their policy documentation - often within seconds of moving off the aggregator site.

Now is your opportunity to verify and fraud screen all the additional information provided after the initial POQ stage.

The ability to enrich the picture of your new customer and carry out checks not available during the quote process (plus doing so in real time) can make or break the relationship with your policyholder regardless of how they come to you – albeit most general insurance policies are now sold via online transactions.

Data enrichment within seconds of policy sale gives you the opportunity to reach out to that policyholder whilst the policy purchase is still fresh and psychologically, they are still in the 'buying' frame of mind.

This narrow window of opportunity means additional premiums can be secured or, if required, the policy cancelled/voided if required with minimal adverse or commercial impact.

Don't forget the middle

This is the area organisations previously neglected at their peril, and not surprisingly is showing growth as an area for fraudulent manipulation.

Mid-Term Adjustments

Fraudsters using compromised identities of genuine policyholders to make a mid-term adjustment to a policy will often do so within days, hours or sometimes minutes of taking out the policy – usually to add on a new named driver or change a vehicle.

With these policies having cleared the original ID&V checks, additional screening is often omitted on mid-term adjustments. Fraudsters know this and target MTAs accordingly. By running real-time checks in SIRA you can see if the new named driver, new vehicle or the amended contact details have been flagged previously as a fraud concern by another member.

These real time checks can all be conducted in the background with no interruption to the customer journey for the genuine consumer and no additional resource requirement on your part.

In addition, the identification of compromised policyholder details gives insurers another opportunity to connect with the genuine customer, protect their interest and build in loyalty.

The end could be much costlier than you'd thought

Taking control of the claims process is critical to reducing your exposure. At every stage there is both a risk and opportunity to identify and prevent fraud.

First Notification of Loss:

Claim details reported at first notification of loss are often limited – particularly in Motor claims where the policyholder may be still at the roadside and in a high stress environment.

It's not uncommon to have only the name, a contact number and the registration number of a third-party vehicle.

But even if the details are scant, check them anyway in real time the moment they are reported to the call centre.

If you have an overnight batch claims screening process in place, the chances are you're not identifying a potential third-party fraudster until after they've contacted a Claims Management Company or, in recent years as fraudsters have adapted their approaches, they have accepted the offers from your own Third-Party Capture/Care team and you've put them in a replacement vehicle, collected their damaged car and started the repair process.

To retract these services a day or more after they have been provided is a costly process that can be mitigated against, at least in part.

Claim updates:

Significant volumes of additional data are provided in the first few days and weeks of dealing with any insurance claim but particularly with motor claims due to the numerous parties and service providers in the supply chain.

If you screened the claimants at first notification of loss stage and found no concerns, **don't assume all is well for the life of the claim.**

— Unscrupulous claimant law firms

— Repairers

— Credit hire providers

— Storage facilities

all play a part later in the claim lifecycle and may not come to light until much later in the process.

Every time a party is added to the claim, **screen them in real time.**

If they're genuine and there are no concerns, the claim will continue unimpeded. If however, there is a fraud concern, you have a fighting chance of spotting it early and can refer it to qualified handler for consideration.

Acting early is the key to reducing and preventing spiralling costs.

Not out of the woods yet

Just because a claim has run smoothly all the way through and looks like every other genuine claim doesn't mean that you can take your eye off the ball.

Claim settlements	Other insurance policies/parties involved
You need to be sure that final settlement payments are going to the correct parties, even where no fraud has been identified throughout the claim process. Once settlements and payment terms are agreed, check that the bank account is valid and has not been linked with previous fraud activity. This check, like all others, takes just a few seconds, doesn't affect the customer journey and can potentially save £££s in losses. If you leave it until after the payment is made, it can be impossible to recover the funds.	Fraudsters traditionally targeted personal injury pay-outs from road traffic accident insurers. Since the Whiplash reforms came into effect, there has been a rise in bent metal and cost layering. While these tend to affect the RTA insurer, don't forget that on vehicles that are less than three years old there is often outstanding finance and a GAP insurance policy in place. Fraudsters have become wise to the value of these GAP policies and may actually be using the RTA policy as a means of securing settlement from the GAP policy.

Many GAP insurers have proven fraud on a theft or total loss claim.

While they've not paid out the claim on the GAP policy, the fraudster has still walked away with the proceeds of the initial claim with the compensating insurer being blissfully unaware.

More is definitely more

Personal Injuries resulting from motor claims remains a core focus for many fraudsters, but many are branching out into areas such as credit hire, storage and recovery for exaggeration of costs.

Historically, claims farmers ran 'Slip and Trip' claims particularly against local authorities but also private sector commercial enterprises targeting their Employers Liability and Public Liability policies.

If you're a composite or large commercial insurer or a broker with multiple lines of business, it makes sense to screen all books for fraud.

A bad actor who appears in one area of your business may well be up to no good in another.

Equally, if you reject a third-party claimant's case for fraud, but they're a policyholder in another area of your business, do you really want them on your books? It could just be a matter of time before they seek, what they perceive to be, 'compensation'.

Making sure all your data is synced to your counter-fraud system is logical for your current needs and will also help future proof you.
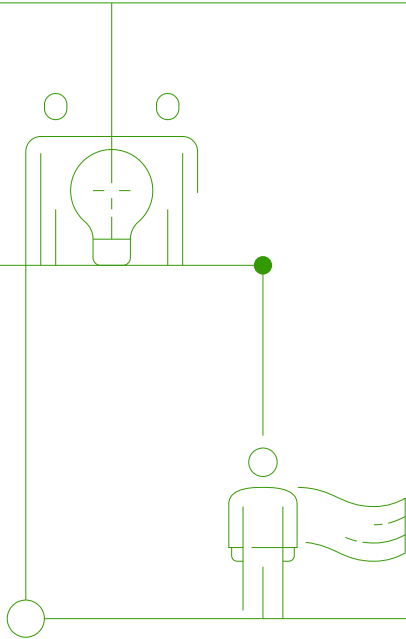
Most solutions allow you to do this at no additional cost.
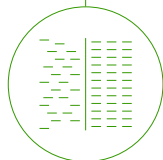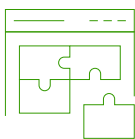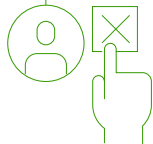
Putting people at the heart of fraud prevention

Although you might not expect us to say this, we are only part of your fraud detection and prevention solution.

It may seem counter-intuitive in today's modern age, with a focus on technology but well trained and motivated staff are key to identifying many types of fraud.

While machines are getting more intelligent, it still takes a human to identify the triggers and flags raised during any interaction with a potentially fraudulent customer. It's only from this that data can be generated for the automated systems to do their work.

Make the most of what you get

As a National SIRA member, you also benefit from a host of complementary services:

— **Monthly thematic calls** to promote and enable discussion of fraud trends, challenges and good new stories with industry peers.

— **Special Investigations Unit** If you've got a suspected fraud trend/MO and want to learn more about the possible industry exposure or, as part of your own investigations you want an intelligence package on an individual of interest then our SIU team can help.

— **Free of charge** rules reviews within your SIRA instance to reduce false positives.

— **A DocuStore** that enables you to append all your documents to a case in SIRA, free of charge. You'll have your complete evidence package in one place, and it's easy for authorised users to access and maintain.

- **Additional update feeds** – the more your SIRA system mirrors your internal system, the better SIRA, Precision and Orion will work.

What does best practice look like?

We're not teaching you to suck eggs here. You probably already have an incredibly sophisticated fraud detection and prevention solution in place. We just want to share what others within your sector – and more broadly across the National SIRA eco-system – have found helpful.

— Where possible, do everything you can in Real Time. With real time responses you can customise and configure multiple customer journeys via Outcome Orchestration, returning real time responses to your in-house systems allowing subtle changes in the customer journey to be effected.

— Seek out as much data enrichment as possible (the right data at the right time) – whether that's via National SIRA or from other sources. Where data is enriched from sources outside of SIRA, send that in as part of your feed where you can use it in your rules, or within Precision and Orion.

You're not charged for sending in additional data items so take advantage.

— When sending data into National SIRA, do so at every touchpoint in the customer journey. Even if the update is minor. National SIRA can always be configured to refer cases only in certain circumstances. Just because you send data doesn't mean workloads and referral volumes will increase.

— Make changes. SIRA, Precision and Orion are all fully customisable. The SIRA system you have today need not be the system you have in 12 months' time. Every time you change your internal practices, want to right a new line of business, take on new business form a different sector or want to change your customer journey – please talk to us. There is always something we can do to assist and we never charge for consultancy.

WE SEE OURSELVES AS AN

extension of your team,

please use us in that way – it's how we know we're delivering the best value for you.

SYNECTICS SOLUTIONS

Tel: **+44 (0) 333 234 3409**
Email: **info@synectics-solutions.com**
Web: **www.synectics-solutions.com**