fraud.com

fcase Fraud Orchestration, Automation & Response

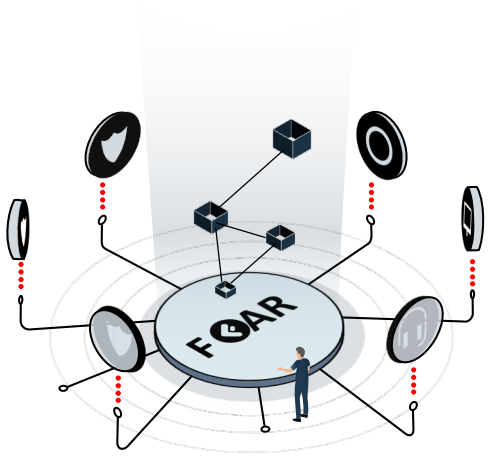
Unite your existing anti-fraud investments to strengthen your defences and improve operational efficiencies

What is fcase FOAR ?

fcase - Fraud Orchestration, Automation, and Response enable organisations to collect and fuse vast amounts of risk signals and related data from a wide range of internal and external sources.

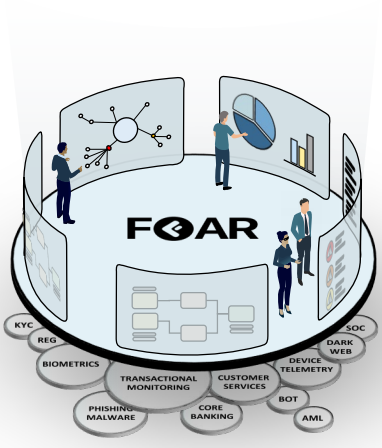
Delivering centralised fraud intelligence and automation on top of your existing anti-fraud investments, improving the efficiency and effectiveness of operations, enhancing incident response, reporting and knowledge capture.

fcase FOAR is the method of connecting fraud tools and related systems, closing the gaps between anti-fraud, cyber, customer services and beyond. It is the combined central fraud layer that streamlines fraud operations, powers fraud automation, manages the customer journey and improves fraud prevention effectiveness.



How is FOAR helping organisations overcome their fraud operational challenges ?

Too often, financial institutions and alike face the challenge of siloed anti-fraud systems and operations with little-to-no cross-functional or departmental communication. For fraud prevention to be effective in the context of delivering the perfect balance between fraud prevention and customer experience, the enterprise must be connected and working in harmony via one final orchestration layer that connects and manages your point systems, such as anti-fraud. ↓



Boosting Customer Experience

With a real-time unified risk & trust assessment approach, organisations can manage the entire customer journey, to improve service & trust.

Unifying Operations

Creating harmony between people, departments, processes & technologies for greater effectiveness & efficiency.

Supercharging Investigations

Work smarter & faster with threat-centric cases & visual threat storylines, improving effectiveness, reducing caseload & magnifying your team's efforts.

Fraud Orchestration - The Silver Bullet…

When it comes to fraud and operations, only a few things are constant and predictable in recent years, more fraud, more complexity, more attack vectors.

One thing is for sure, the more data points connected, gaps closed, via one final overarching agnostic layer, the more ability to manage and reduce fraud while improving customer trust and lowering operational costs. fcase FOAR transforms your most significant fraud operational challenges into superpowers for your organisation, which all starts with the most critical asset [Data].

Data Collector

To enable a single source of the truth and empower your operations, as a first step, fcase FOAR data collector, **collects (↓), aggregates internal and external risk signals ●, transactions – events ●, and customer data ●** from your existing systems via flexible parallel real-time processes.

Further to data collection, the data collector serves as a **data gateway** via APIs or flexible plugins. Firstly issuing messages and actions ● to the core banking system such as hold card until risk removed, or an action to customer services. Secondly **Providing enriched ● cleansed data back (↑)**, to enable risk systems to improve their machine learning, or new services to assess and score clients in a more defined way, or empower customer services, regulation and marketing to make better-informed decisions.

Data Fusion

With a single source of the truth fraud layer, FOAR data fusion begins to **create a unique view of the customer**. The key is to do this in real-time at the point of data collection.

FOAR data fusion **forms a central, clean, connected and accessible fraud intelligence data hub** that presents a collective intelligence across the organisation.

Threat-Centric

FOAR threat-centric changes fraud operations paradigm by **focusing on threats, not just signals** on their own, each independently. FOAR threat-centric continuously analyses risk signals and associated data, identifying commonalities indicative of a coordinated attack - the threat / the risk timeline.

For each threat, FOAR threat-centric gathers all the insight you need, **reducing investigation research by up to 80%, force-multiplying your operations, reducing fraud, improving efficiency and customer trust.**

Fraud Orchestration: **Automation**

A common fraud management shortcoming within many organisations is the lack of centralised fraud coordination across multiple fraud prevention, core and operational systems. This shortcoming typically results in higher fraud, false positives, good customers getting declined, fraud operations inefficiencies coupled with higher prevention and operational costs. With fraud orchestration and automation together, organisations can close the gaps fraudsters exploit and manage fraud efficiently and effectively using a unified, cleansed single source of the truth coupled with Robotic Process Automation (RPA) in the form of playbooks. Playbooks are defined via simple drag and drop trigger, condition and action blocks using the codeless workflow designer. With FOAR organisations can ↓

Reduce Repetition

Free investigators to apply their skills on higher-value work by **automating repetitive tasks**, from creating - closing & updating cases, updating customers & customer services on investigations, to performing actions such blocking, unblocking services and so much more. RPA tasks improve operational effectiveness, with efficiencies & customer satisfaction

Reduce False Positivises

False-positives are an annoyance to any operational team; they divert attention away from dealing with the real threats while reducing customer trust. Fraud automation can classify and **close false positives as the final united risk layer without the need for fraud investigators** input. Fraud investigators can now focus on the threats that genuinely need their attention and expertise, reducing fraud and improving trust

Enable Auto Decisioning

Model, manage and automate repeatable business decisions pre & post events. From assigning - escalating cases, setting tasks, managing customer authentications, setting limits, obtaining data, to storing results of one playbook for another, E.g. Fraudulent scenario on mobile, use that mobile for another playbook. The scope is limitless to reduce human error, improve efficiency, enable consistency & close gaps

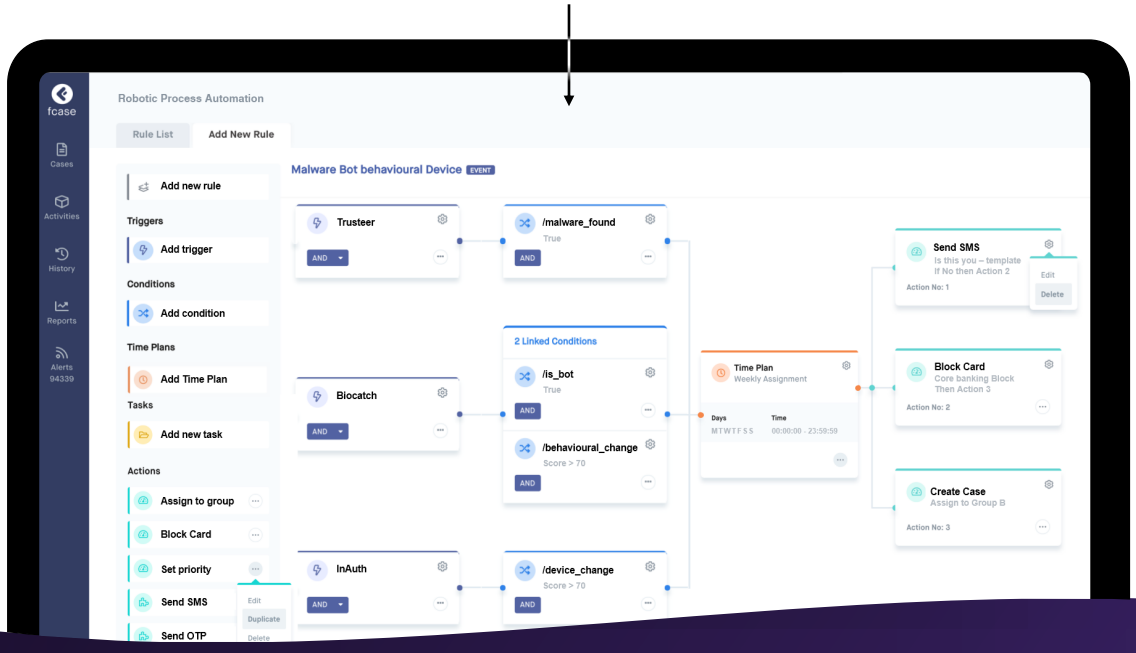
Orchestration, Automation in Action

Fraud Attacks are coordinated, and evolve in the most unpredictable ways, while anti-fraud systems are uncoordinated due to their siloed nature; however, when united into one final layer, the real potential shines through.

In the following example below, a customer makes a transfer of funds using their online banking App. The App first checks for risks, via several fraud SDKs embedded within its APP. fcase automation assesses the customer journey in parallel as a final layer, binding the risk signals across all systems orchestrated delivering an outcome in real-time. For example, Malware + Bot + New Device + behavioural change = Send authentication to the client (using the known mobile number), wait for x for a response, if No then Block card (or Hold card until response) and create a case.

Other examples to name a few:

- Notify KYC of risk on an entity
- Close case based on x, update client
- No OTP sent after x, send another
- Set severity based on x scenario(s)
- On x date send fraud report to x
- Manage a customer complaint
- Request a refund, update client after
- Set task, review incorrect risk signal(s)



Response: **Fraud investigations, Remediation**

Fraud investigations form an integral process within the fight against fraud, not only focusing on risk signals but also liaising with the police, crime agencies, cognitive interviews with customers, internal business inquiries and so much more. Understanding the fraudsters steps is always a challenge, especially when most of the data required is across a myriad of anti-fraud, transactional and customer systems. Fraud investigators spend on average about 60 to 80% of the investigation process gathering data, and the remaining on the fraud cases itself.

The main problem in fraud investigations when investigating cases is the absence of threat coordination. For example, investigator one is focusing on a malware risk signal, and investigator two is focusing on Bot attack, investigator three is focusing on a money transfer, while investigator four is focusing on a change of device. Each investigator does not know the full picture from the outset, or their colleagues are working on common cases to their own. This approach leads to false positives, reduction in customer trust, investigator fatigue and is incredibly inefficient and costly.

Threat-Centric Cases

The fcase case manager module forms a common investigation platform across all your point systems such as anti-fraud and Cyber. One final layer delivering a full picture of fraud, conducting the research and presenting the results automatically by threat. This, in turn, improves investigation accuracy and operational efficiency up to 9x.

For every threat, **fcase FOAR case manager presents all the data and combined tools needed to remediate with extreme efficiency**. ↓

1 Common cases

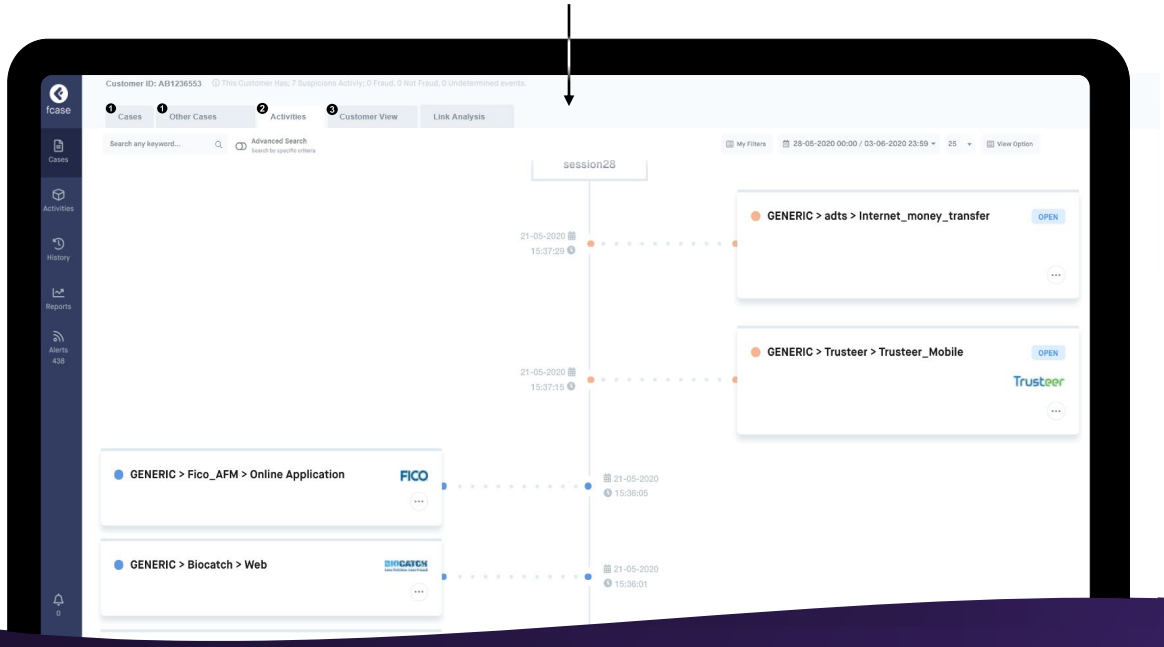
All internal risk signals, transactions, events, customer data and external sources for a particular threat, presented into one case via flexible data widgets. This powerful insight driving rapid decisions. All cases have history, notes, files, actions and can be exported.

2 Threat Storylines

Get a visual story of the threat across time. Search by keyword or conduct advanced searches, create and save filters, change views and groups by session. Storylines help your investigate across your organisation with ease.

3 Customer view

A flexible dashboard, aiding investigation to understand a little more about the clients past and current behaviour, from case/activity, account statistics, geo-location to cards and devices used. The more you know the easier to decide.



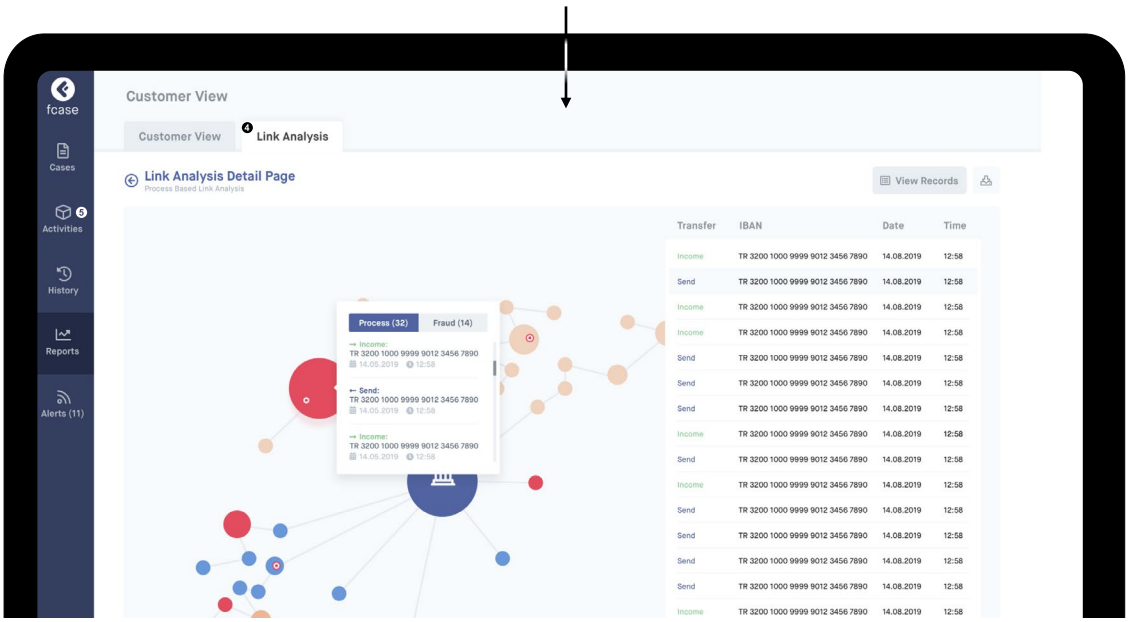
Response: **Link Analysis for Fraud investigations**

In any crime film, there's always a scene when the detective creates a detectives wall full of suspects, locations and dates all connected with string. The detective usually stands back and pieces together what has happened using all the evidence. Link analysis is the detective's wall for fraud, delivered via a graph network, presenting all the evidence across a threat in a visual form so that you can join the dots between the fraudster all its connections.

What connections can be uncovered

Fraud-rings, Synthetic Identifies, Account takeover, online payment, promotion abuse, refund abuse and so much more.

fcase Response Link Analysis can display connections between any data points collected, fused and mapped; therefore Link Analysis for fraud investigation is at its most powerful via fraud orchestration.

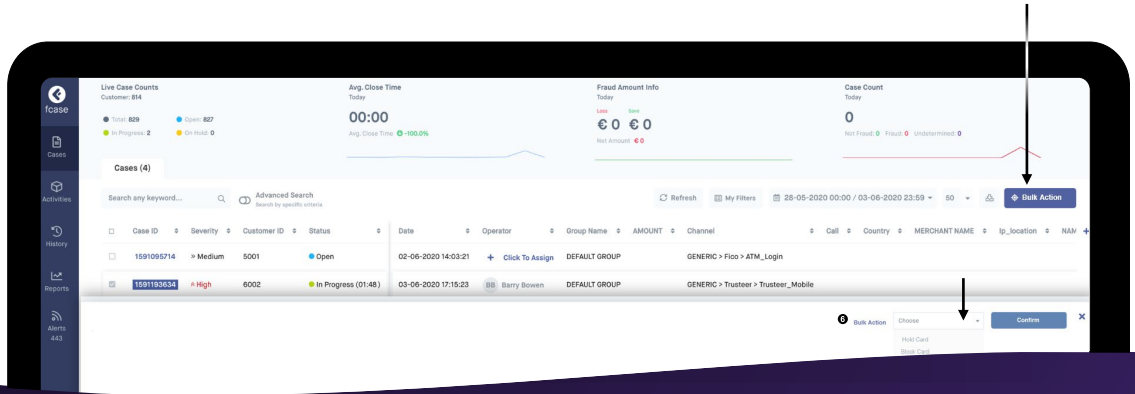


Response: **Search⁺**

Search any condition across risk signals, transactions, events, customer data over time. Create and save personal or global filters, design ticket queue's, and export.

Response: **Actions**

Apply default actions within threat-centric cases or across ticket queues of any condition, such as close - assign tickets, change groups, or design flexible plugins, such as to block - hold the card, issue SMS, send a letter.



Fraud Reporting – **KPI's**

Understanding the full fraud risk across an organisation is a significant task. With fraud orchestration uniting and cleaning your data, reporting on fraud risks, how the team and individuals are performing comes as standard. Below is a brief view of the four main reporting groups, each can be filtered based on your criteria, and each can be download. ↓

Fraud

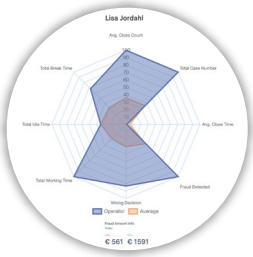
Fraud report by types across time, detailing amount lost, saved by country, teams, channels, …

Efficiency

Visualise your investigation teams performance across time and plan resources

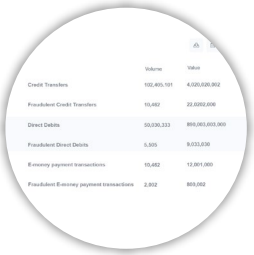
Performance

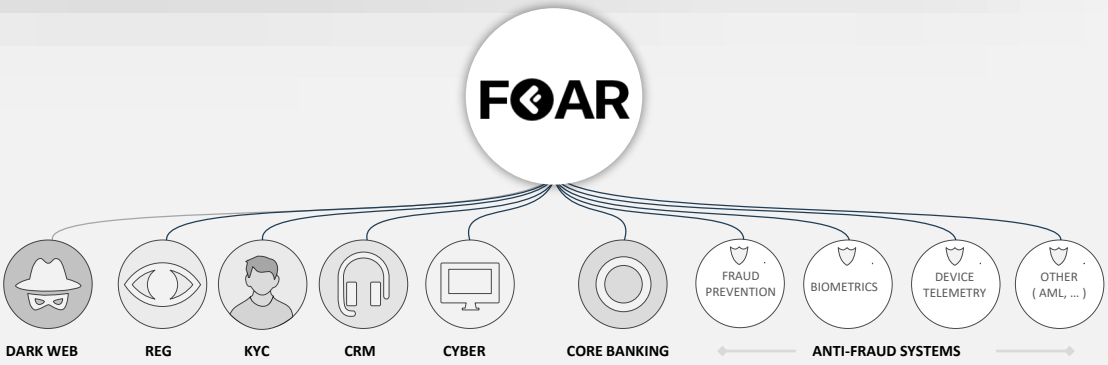
Investigators performance over time, from lost, saved amount, fraud found, wrong decisions, …



PSD2

PSD2 compliancy report, detailing volume & value of service & associated loss





Be the orchestrator, not the orchestrated…

FOAR is not a fraud prevention system; FOAR unites them. Enabling you to work smarter, faster and strengthen your defences, closing the gaps fraudsters exploit, presenting the risks you cannot see, automating tasks, removing repetition and managing the customer risk throughout their journey. FOAR enables you to see more, do more, for less - much less.

FOAR is your fraud defence foundation, wall, hub for fraud prevention, connecting, managing your point solutions. FOAR operates on-premise, cloud or hybrid across a single, distributed, virtual or container architecture. Swap your point systems in and out as you desire. The more point systems connected, the more collective insight with efficiencies gained.

fraud.com

fcase FOAR is your home for fraud operations, equipping you with the visibility, analytics, and automation you need to unite your teams and amplify efficiency.

What can you do with fcase FOAR?

Contact a specialist