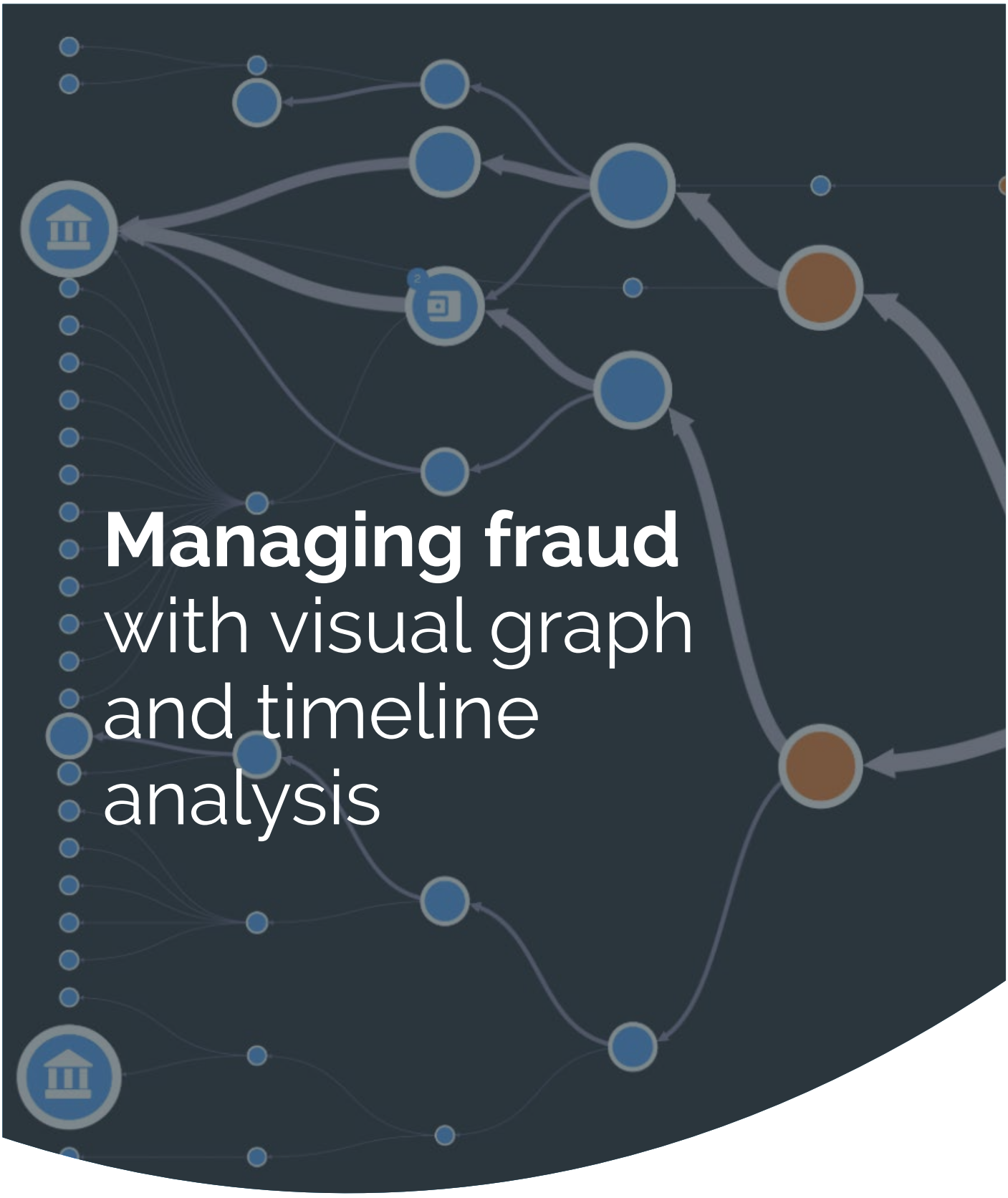


Managing fraud with visual graph and timeline analysis

Cambridge Intelligence

Contents

Fraud as a graph challenge

Fraud is an expensive problem. It costs the global economy over US$5 trillion annually, and each dollar lost conceals $3.75 in additional costs created by detection, investigation and prevention.

It's an increasingly complex challenge, too, with new digital technologies and services creating additional opportunities for fraudsters to commit crime quickly, remotely and through increasingly hard to detect methods.

Understanding data allows organizations to detect, investigate and prevent fraud more effectively. Visual graph analytics - sometimes known as link analysis - combined with timeline analytics makes that possible.

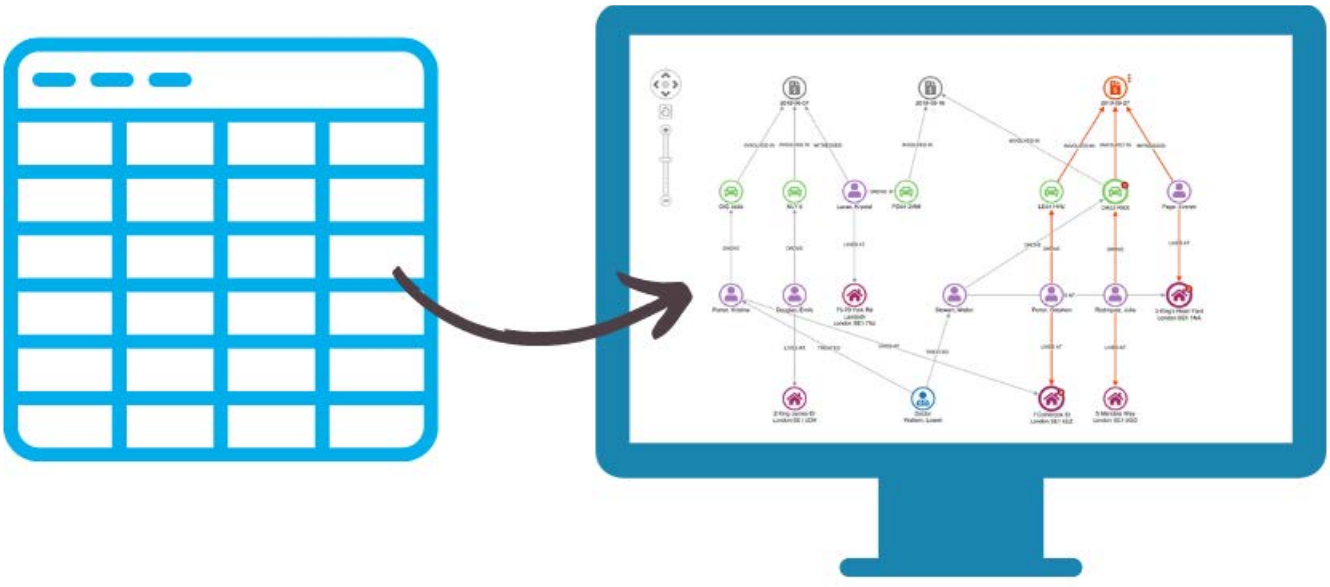
The examples in this white paper use simplified and synthesized data, but they represent real fraud management workflows. We've focused on specific types of fraud, but the techniques apply to any scenario where individuals need to understand transactions and activity over time.

For more examples of how our tools help organizations manage fraud, take a look at our blog.

What is visual graph analysis?

Visual graph analysis is a data visualization technique for making sense of connections and relationships.

When an event occurs - a financial transaction, an insurance claim, a login to an online banking system - it creates a digital footprint. Using visual graph analysis, fraud analysts and investigators visually connect those footprints as nodes and links to uncover unusual patterns that indicate fraudulent activity.



Visual graph analysis helps analysts to interpret and understand huge volumes of data, fast

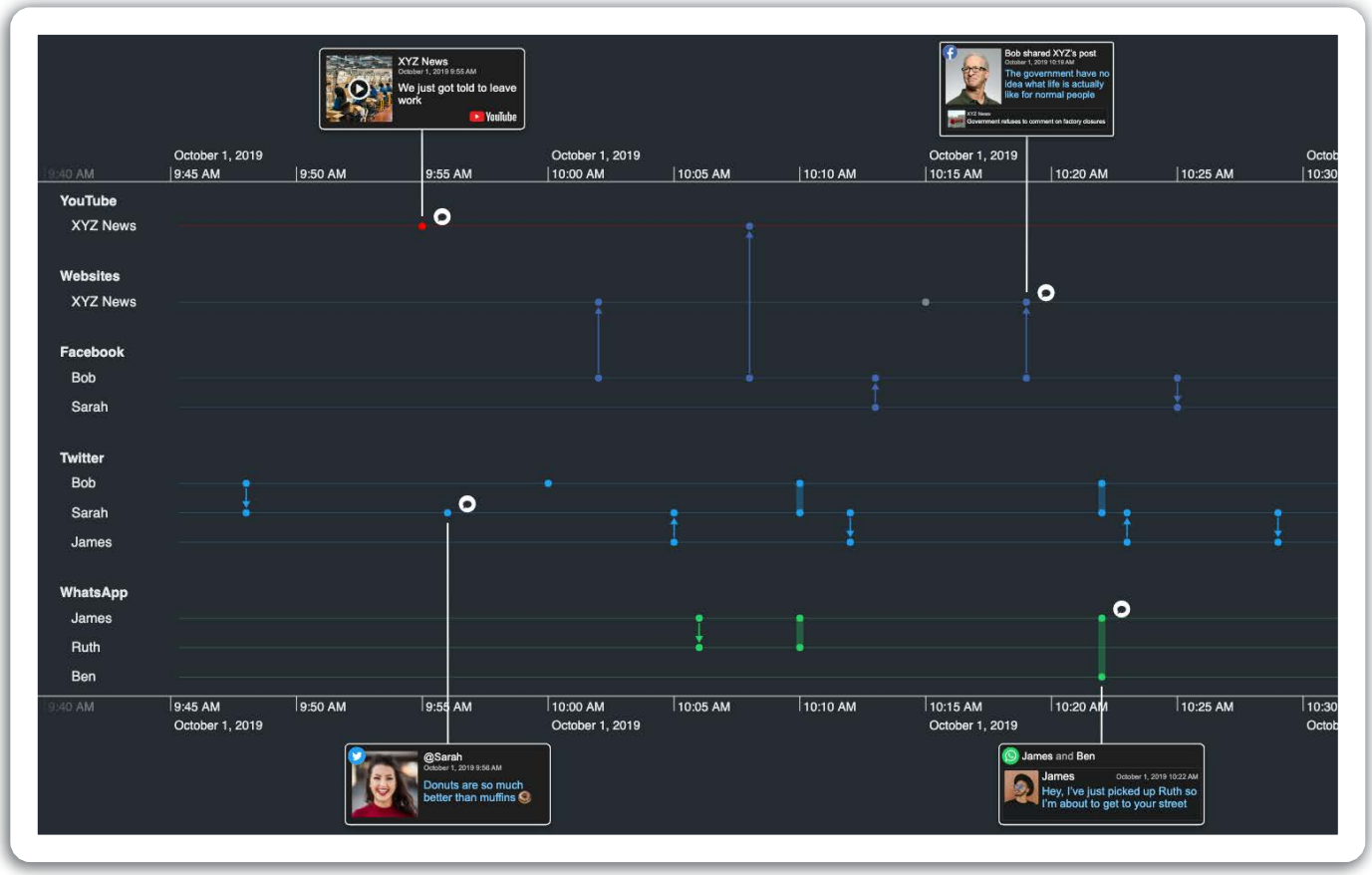
Visual graph analysis isn't new. Law enforcement and financial services organizations have used the technique for decades.

The tools involved, however, have improved significantly over time. Growing data volumes, changing fraud methods, and increasingly distributed analyst teams have driven a new generation of web-based, fully customizable tools.

What is visual timeline analysis?

Visual timeline analysis is a data visualization technique for exploring how time-based events and activities evolve.

Timeline charts show digital footprints over time in a scalable and interactive way. They can be combined with visual graph analysis charts, or used stand-alone. In either case, they show analysts when events happened, and how they were linked.



An example of a timeline visualization, showing events over time

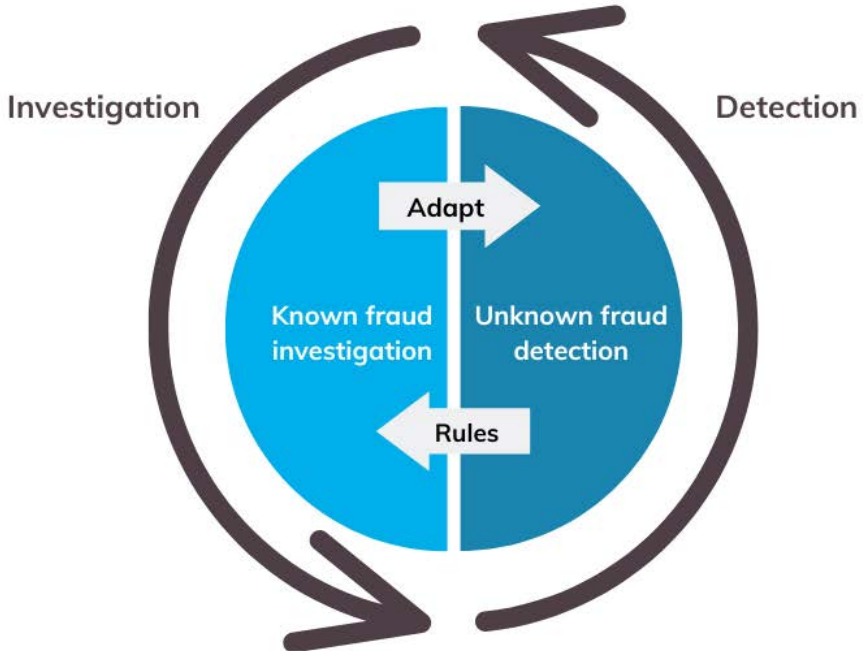
The fraud management process

We can broadly define two categories of fraud: known fraud and unknown fraud.

Known fraud is fraudulent activity that's been seen before. Organizations can define the behavior patterns involved and detect them automatically with rule-scoring and pattern-matching. In this scenario, visual graph and timeline analysis act as a fraud investigation technique. They're a fast and reliable way to manually review or investigate borderline cases that cannot be resolved automatically

Unknown fraud is fraudulent activity that doesn't follow a familiar pattern, so automated processes won't necessarily spot them. It requires human intervention to identify new or unusual patterns. Here, visual graph and timeline analysis becomes a **fraud detection** technique.

Insights gained from 'unknown' fraud detection feed into the automated 'known fraud' rule-scoring and pattern-matching processes, resulting in a more robust and accurate fraud management regime.



Insight from unknown fraud detection feeds directly into known fraud investigation processes

Let's take a look at an example from each category, to see how visual graph and timeline analytics improves the speed and robustness of the process.

Reviewing and investigating known fraud

When an investigator looks for known fraud patterns, each case is automatically scored and assigned to a category, for example:

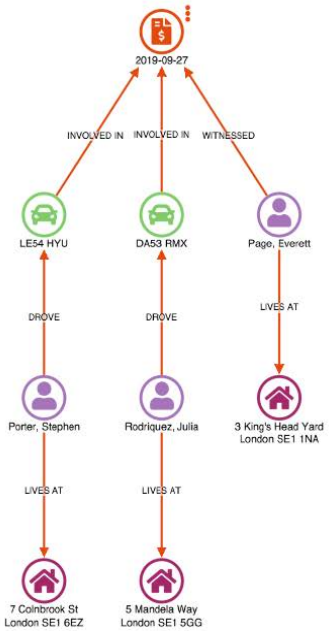
- **Legitimate transaction - allow**
- **Flagged transaction - review**
- **Fraudulent transaction - block**

When reviewing flagged transactions, volume and speed is critical. Customers expect decisions quickly - often in minutes for some online transactions. Analysts need to understand the situation, make an assessment, and close or escalate the case quickly without letting fraud slip through.

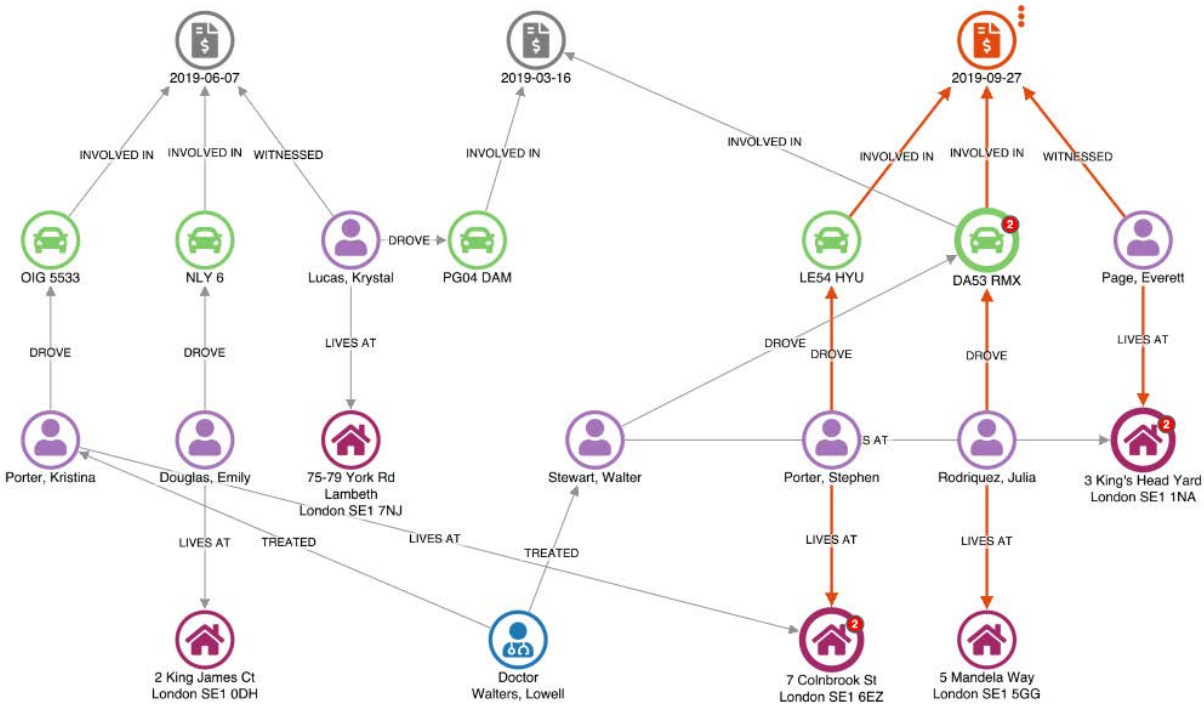
Visual graph and timeline analysis powers that process. It provides an intuitive way to quickly understand a case and its flags.

Insurance fraud detection

Here's a visual graph analysis chart showing a vehicle insurance claim, flagged for review. Nodes represent claims, vehicles, people, and addresses. An automatic hierarchy layout makes it easy to spot dependencies.



Let's see if this claim shares any attributes with previous claims. A quick database call draws in two further claims.



Our chart shows a blue 'doctor' node connecting two claimants. Nothing especially unusual there.

We also see two claimants that live at the same Colnbrook Street address. Their shared surname suggests a family relationship which, again, isn't unusual in itself.

But we also see a vehicle - registration number DA53 RMX - is connected to two claims just 6 months apart. For one vehicle to be involved in two claims in such a short space of time is unusual, so it's flagged for further investigation.

Advanced visualization, embedded in the analyst workflow

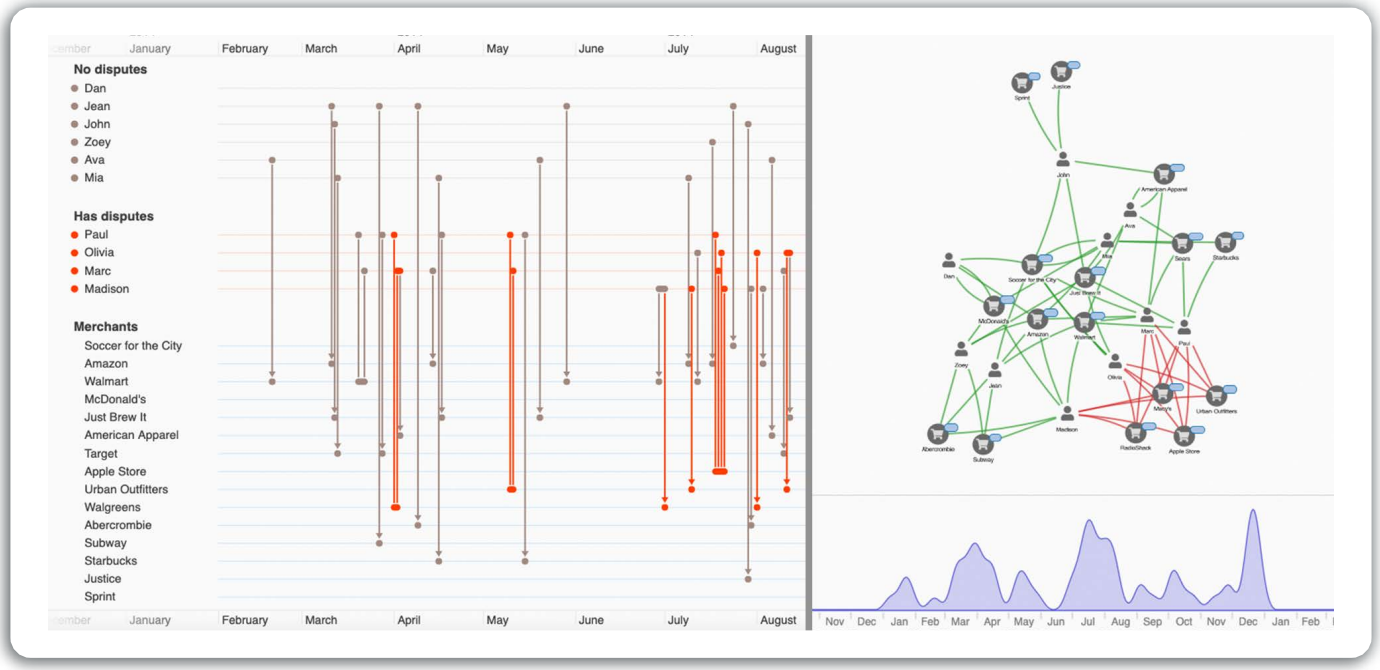
To make fast decisions, fraud analysts follow efficient workflows.

With our graph and timeline software development kits (SDKs), developers can create visualization components, fully customized for a specific workflow, and embed them directly into existing products and platforms.

The result: analysts get advanced visualization, without switching tools or disrupting their flow.

Revealing suspicious credit card activities

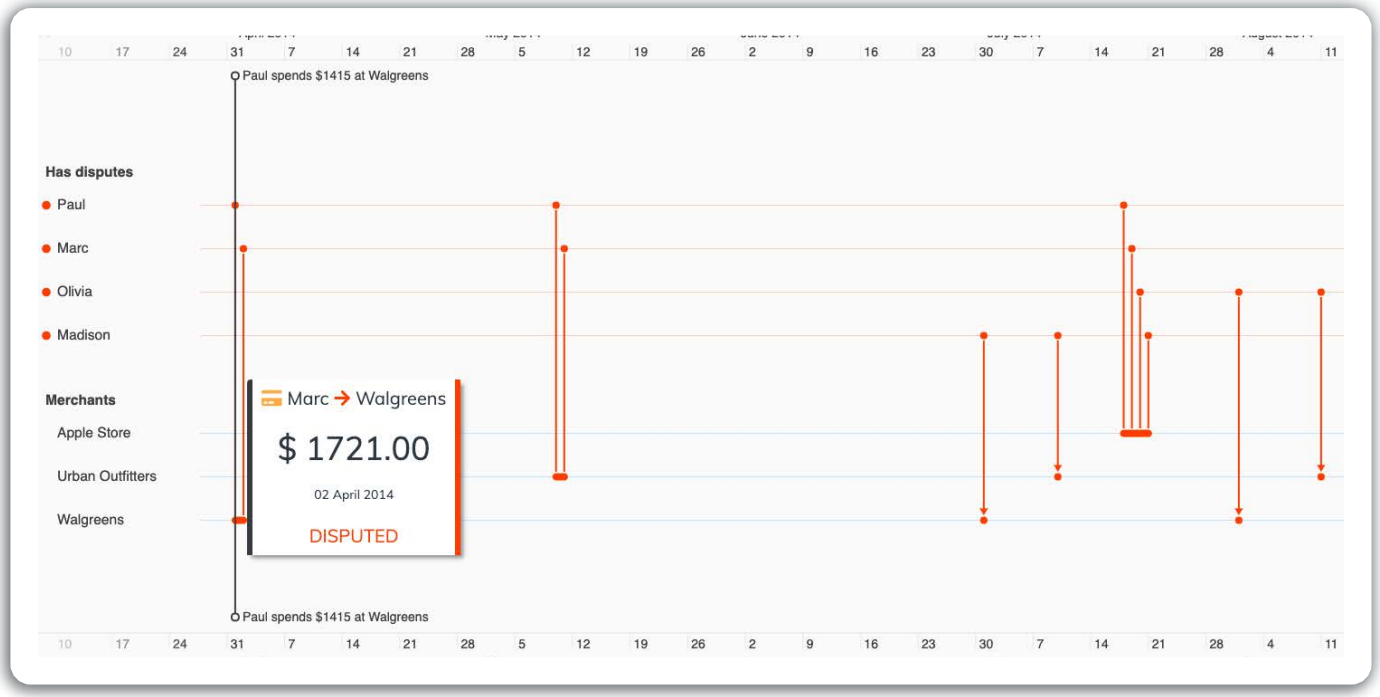
Visual timeline analysis helps when the sequence of events is determines the legitimacy of transactions. Here, for example, we see a set credit card transactions presented as both a graph and timeline:



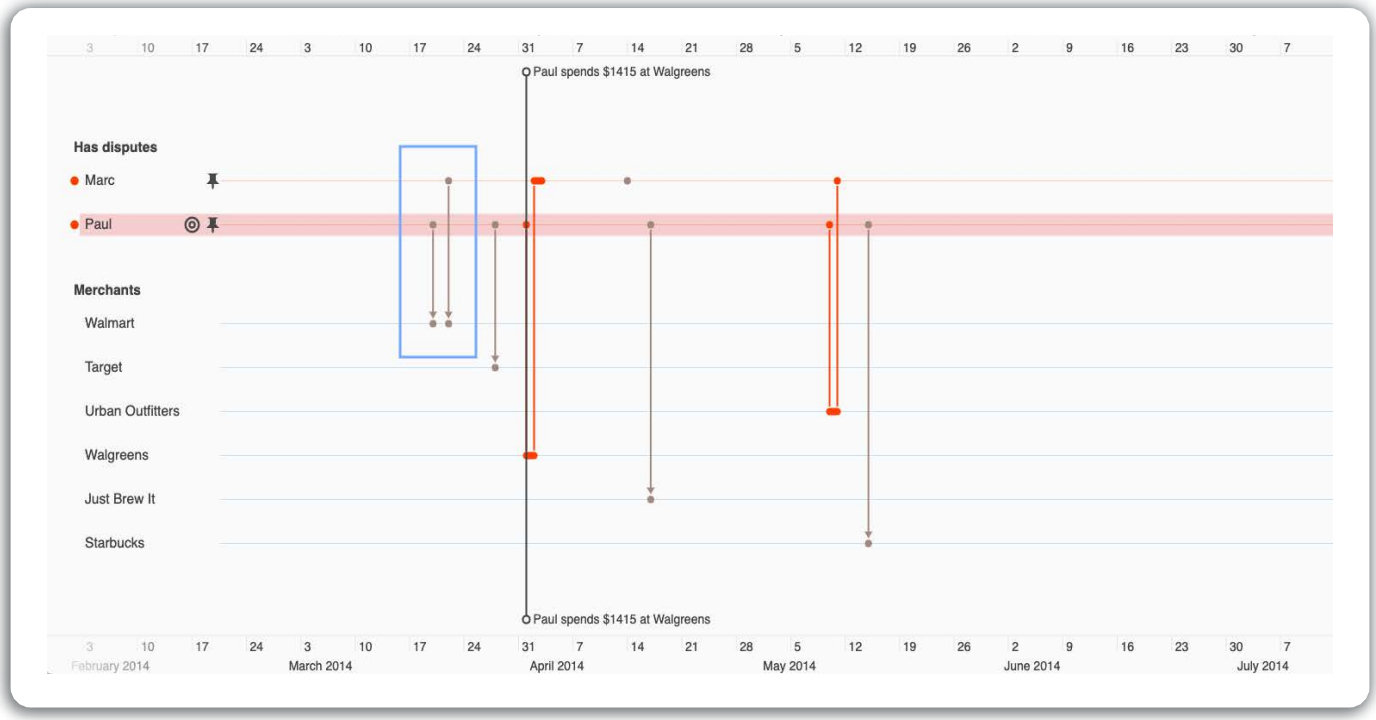
Links (in the graph) and events (in the timeline) represent transactions. Red links and events are blocked transactions. Nodes (in the graph) and entities (shown down the left-hand side of the timeline) represent people and merchants.

Both views show a set of disputed transactions, starting around April. We spot the first disputed transaction - a $1415 payment from Paul's credit card at Walgreens on 01 April - and add a marker to highlight it.

For a clearer view of the extent of the problem, we filter the chart to look at just the disputed transactions. We see Marc also disputed a transaction at Walgreens the following day:



Finally, let's pin both Paul and Marc to the timeline, to focus on their activity, then remove the filter so that we see every transaction again. This reveals that they both visited Walmart in late March. Were their cards cloned there?



These simple examples show how visual graph and timeline analytics provide an intuitive and fast way to explore complex sets of transactions. It means analysts can uncover unusual patterns that might otherwise get overlooked.

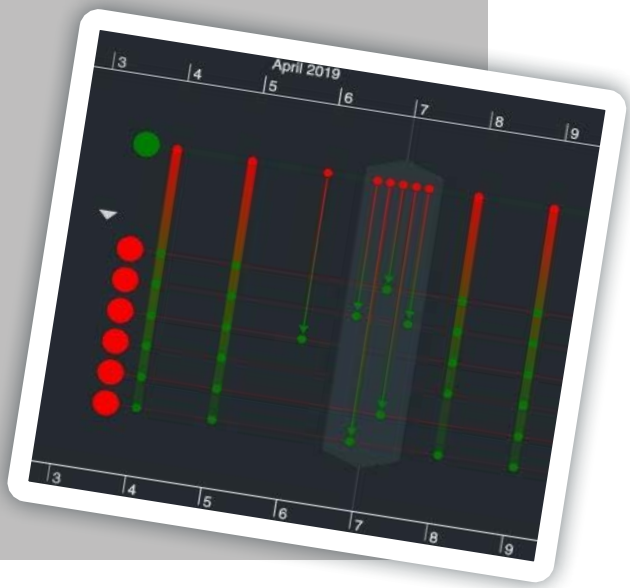
Visualizing complex transactions

Financial investigations are rarely simple.

They involve thousands of transactions, often in quick succession, between multiple parties.

KronoGraph, our visual timeline analysis SDK, offers techniques to help investigators make sense of the most complex transactions, without overwhelming them.

The result is clear timelines that power a user-led, exploratory approach to investigations.



Detecting unknown fraud

The previous examples show how visual analytics help in cases where a flag has been raised already.

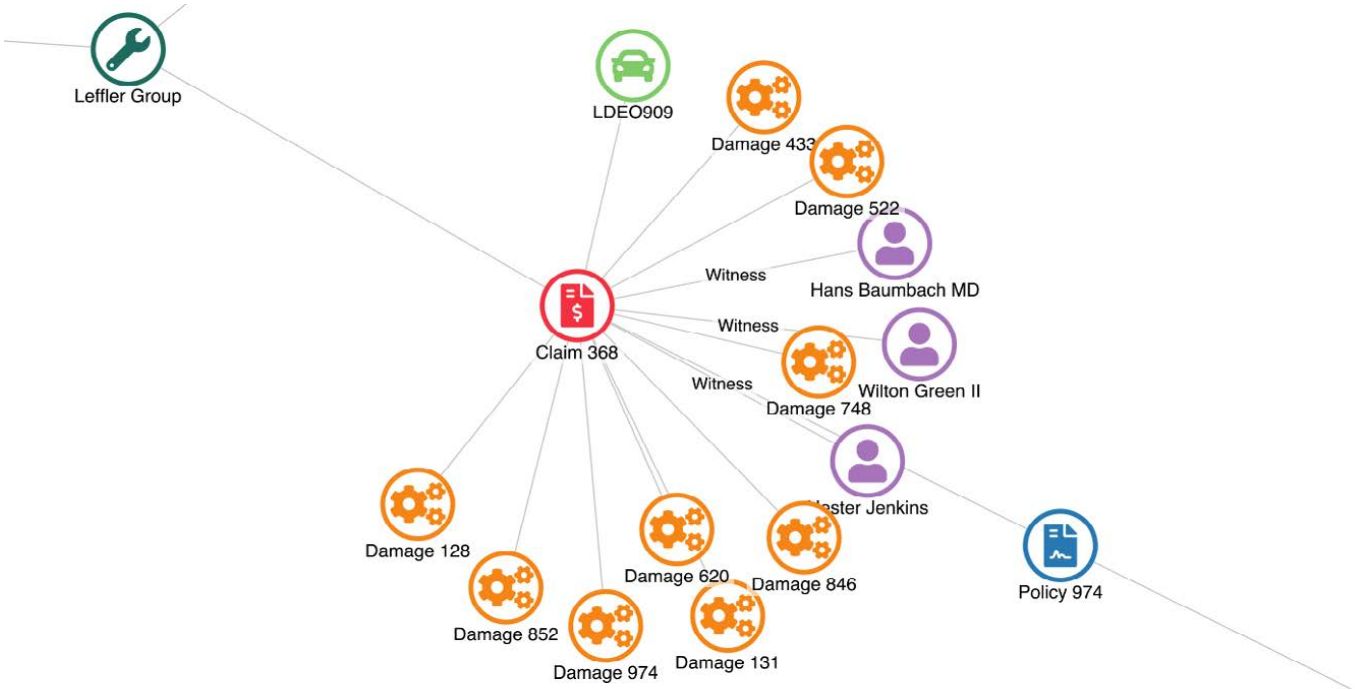
But what about fraud that goes on under the radar? To identify that, analysts use domain knowledge and experience to think like a criminal. They must anticipate new tactics to commit fraud and hide it from authorities. Again, visual graph and timeline analytics is an essential technique.

Reviewing and investigating known fraud takes a case-centric (or local) approach - it starts from a specific point and works outwards. Detecting unknown fraud requires a global approach - it takes an overview of a large amount of data to find anomalies.

Unmasking the scammers

This example tackles vehicle insurance fraud in a different way. The fictional but typical dataset includes links between nodes representing policies, policyholder details, insurance claims, vehicle damage, doctors, witnesses, and mechanics.

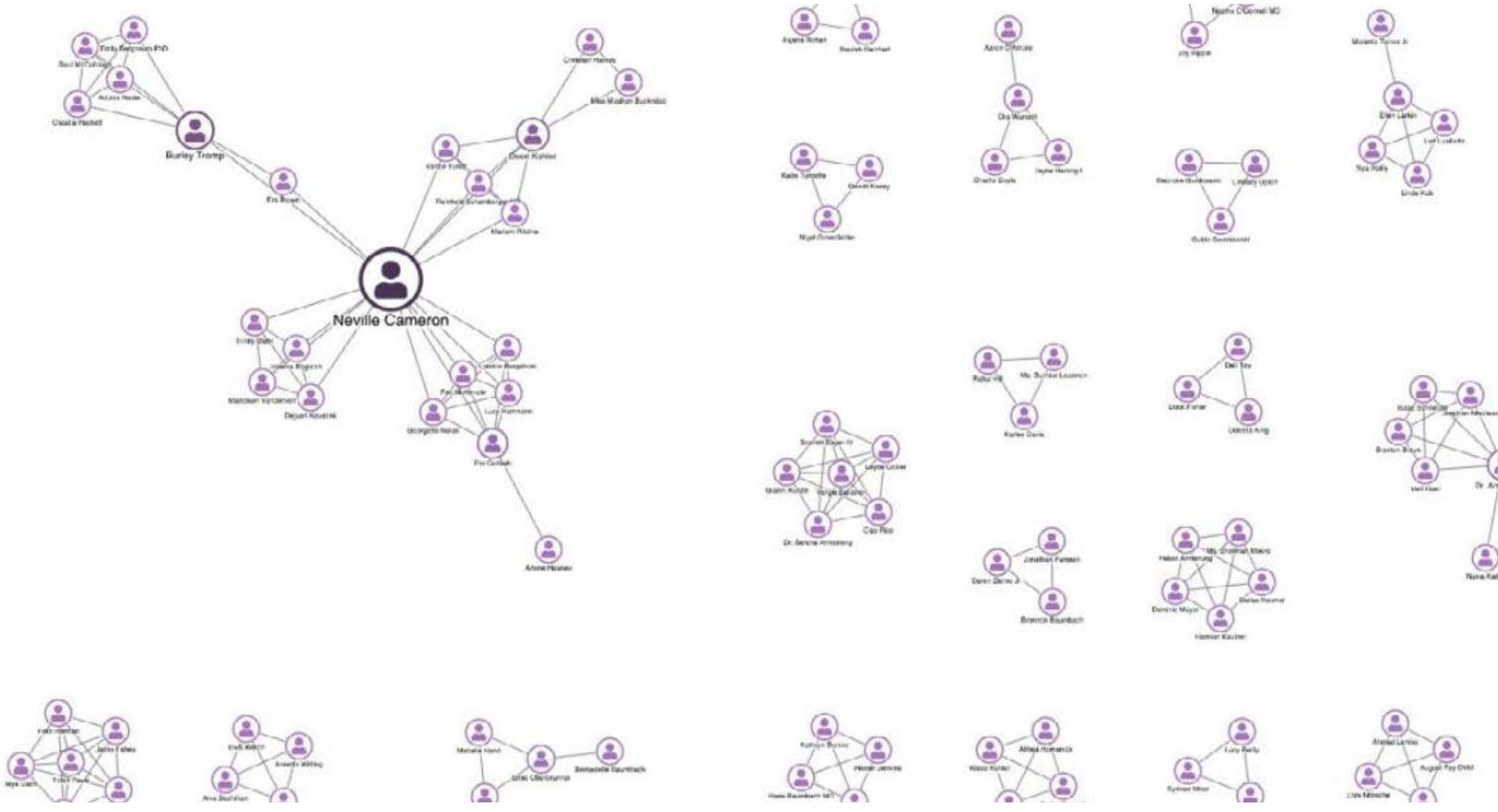
When you visualize many cases in one chart, it's easier to spot ordinary claims (the Y-shaped structures dotted around the chart). It also highlights more complex, or potentially fraudulent, claims.



This claim on a single policy contains nine separate damage claims

Spotting unknown fraud relies on the analyst's domain knowledge and powers of investigation, enhanced with visual analysis.

We can simplify the view above to show people who share 1st or 2nd-degree connections through claims and policies. This reveals people involved in multiple claims. At the same time, we apply a social network analysis centrality measure to highlight the most well-connected people. This reveals Neville Cameron as a person of interest:



Larger nodes represent individuals linked to multiple insurance claims – legitimate or fraudulent

Cutting through noisy networks

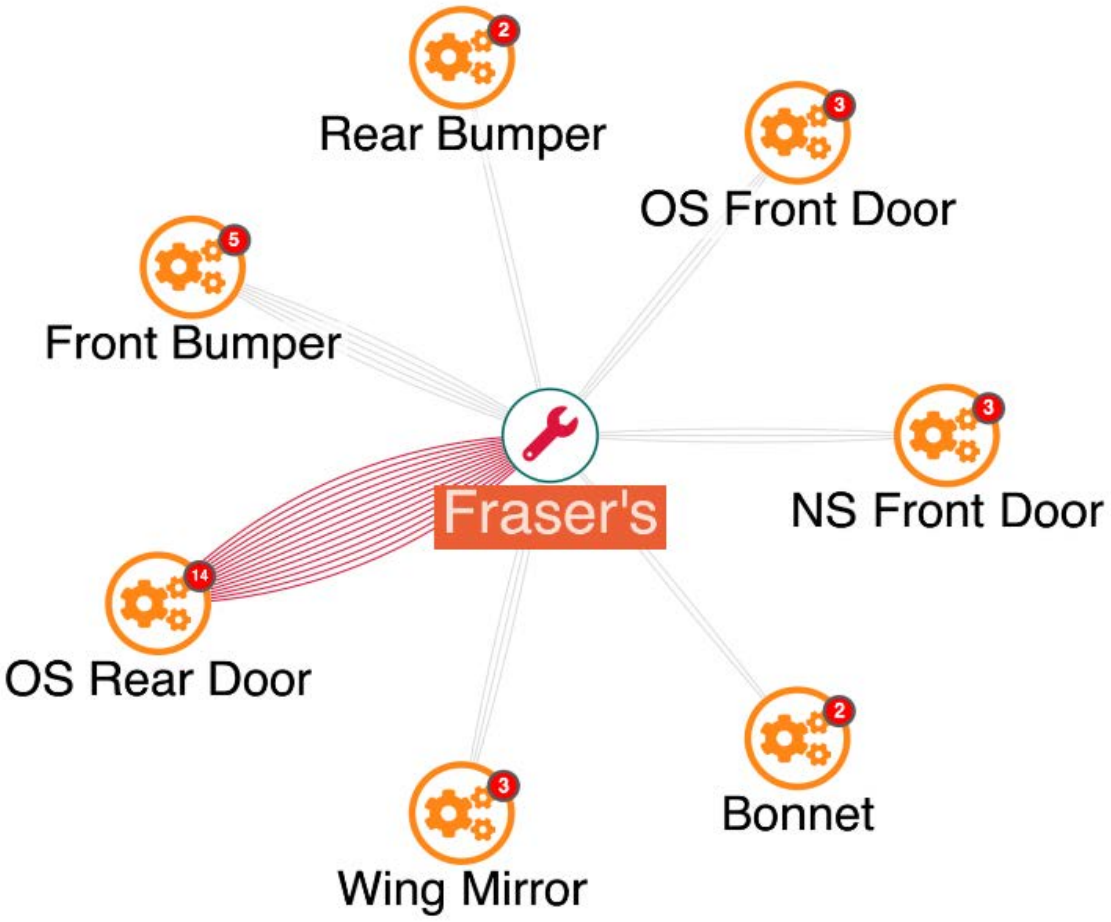
As fraud investigations grow, investigators can quickly become overwhelmed by the volume of data they need to understand.

Our SDKs offer a range of tools to eliminate noise leaving users to focus on the nodes and links that really matter.

With the help of filters, social network analysis, powerful automatic layouts and smart node grouping, investigators can find the answers they need.

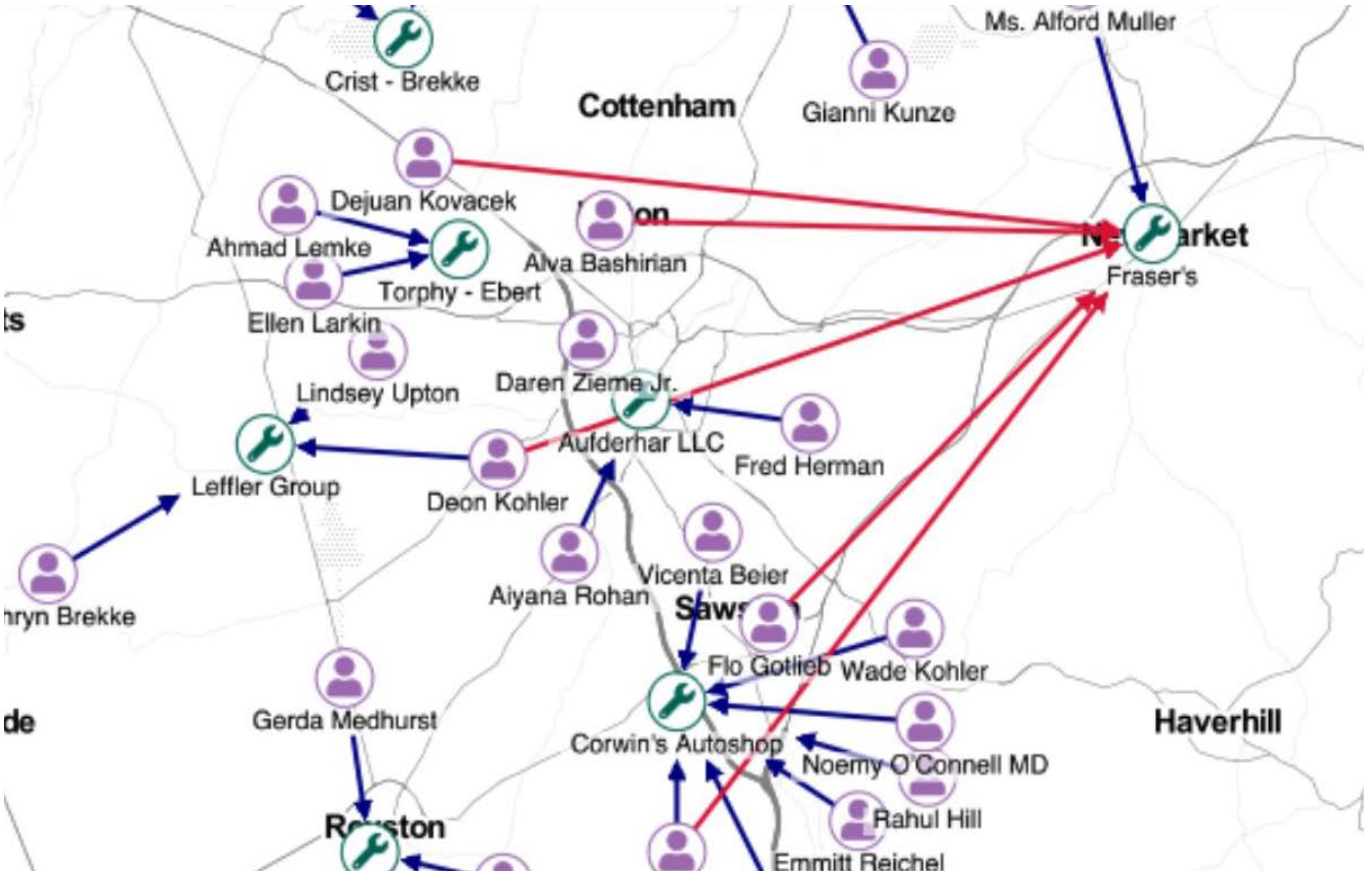
Learn more about techniques for visualizing large graphs.

Let's take a closer look at the damage repairs listed in a claim. Some types of vehicle damage are more common than others. One mechanic fixing a disproportionately high number of similar issues could be a sign of claim inflation - a common fraud tactic where policyholders claim for more damage than actually occurred.



Here we've grouped damage claims by type, and it shows a high number of off-side rear door repairs happening at Fraser's.

Let's plot this suspicious activity on a map to see how policyholders are connected to the mechanics listed in their claims:



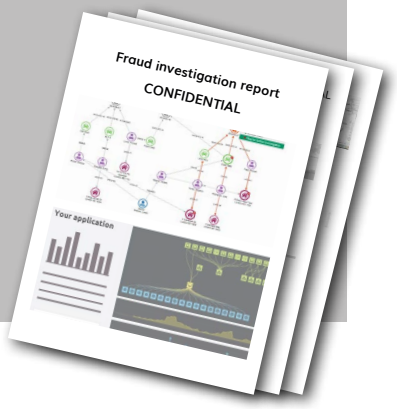
From our analysis of damage types, we know Fraser's was associated with an unusually high number of claims involving one specific vehicle body part. This map view shows that several claimants traveled significant distances for repairs at Fraser's, even though there were mechanics much closer to home. Could Fraser's be involved in an organized scam?

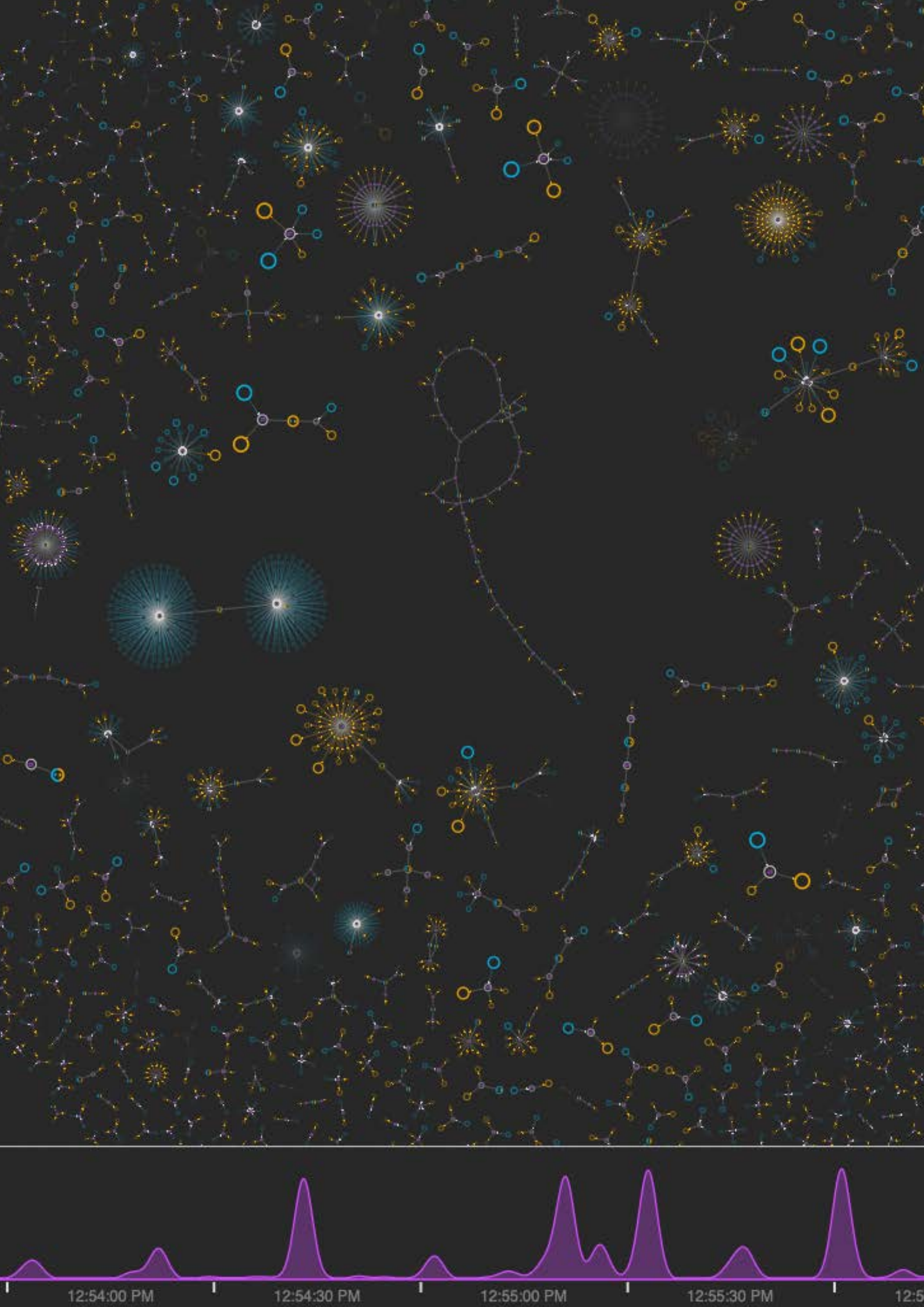
Flexible visual graph analysis drives this investigative approach so that analysts can follow their instincts when detecting unknown fraud.

Disseminating intelligence

Intelligence dissemination is a key stage in a fraud management workflow: sharing the right information with the right people at the right time.

All our SDKs make dissemination easy. Users can share their visualizations, either as interactive charts for colleagues, or as static images or PDFs to submit as evidence.




12:54:00 PM
12:54:30 PM
12:55:00 PM
12:55:30 PM

Unpicking fraud rings, and ‘follow the money’ investigations

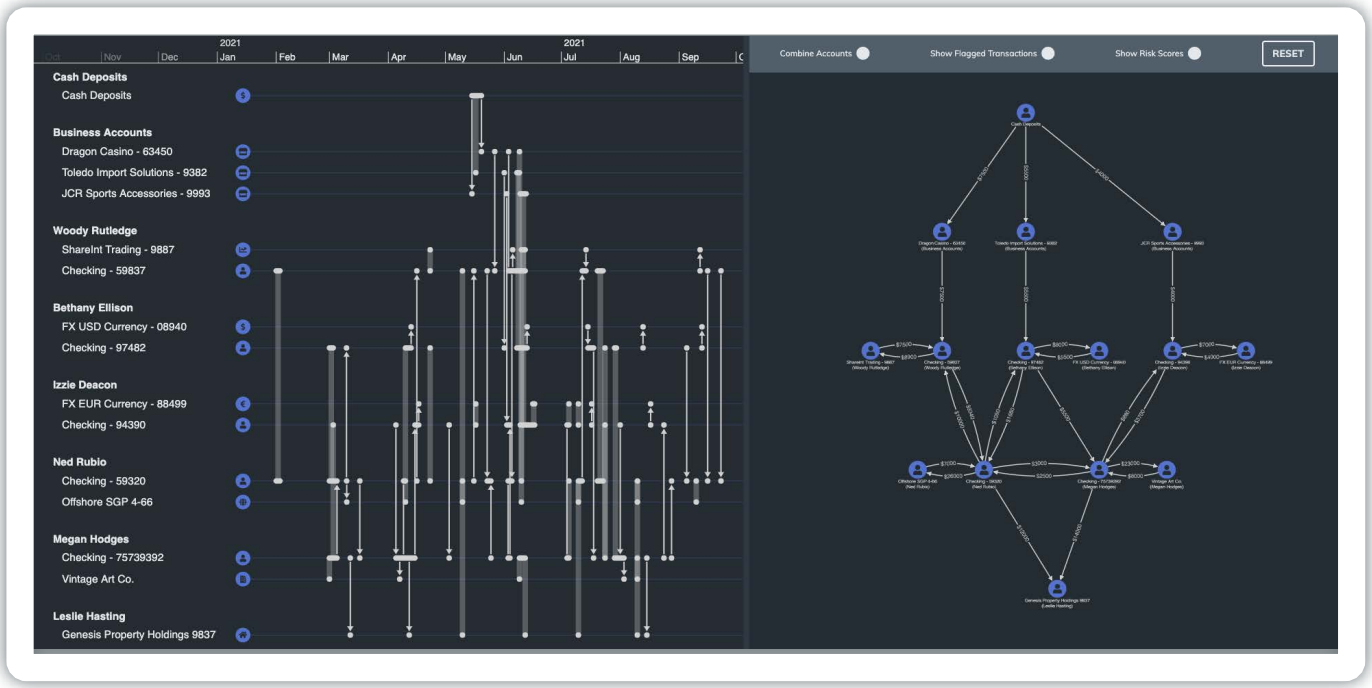
Sometimes fraud cases are standalone incidents - one-off crimes committed by individuals trying to gain some quick cash. Often, however, they’re part of a wider pattern of activity.

Organized criminal gangs work together to commit fraud, and launder the proceeds from it, and use multiple accounts to conceal their activity within complex webs of transactions. Investigating these rings is especially complex, as they involve large numbers of accounts mixing illegitimate and legitimate-looking transactions. Failure to spot fraud rings leaves organizations exposed to further fraud losses, and gives criminals opportunities to launder money through legitimate financial facilities.

Let’s see how visual graph and timeline analysis helps investigators unpick fraud rings with a ‘follow the money’ investigation.

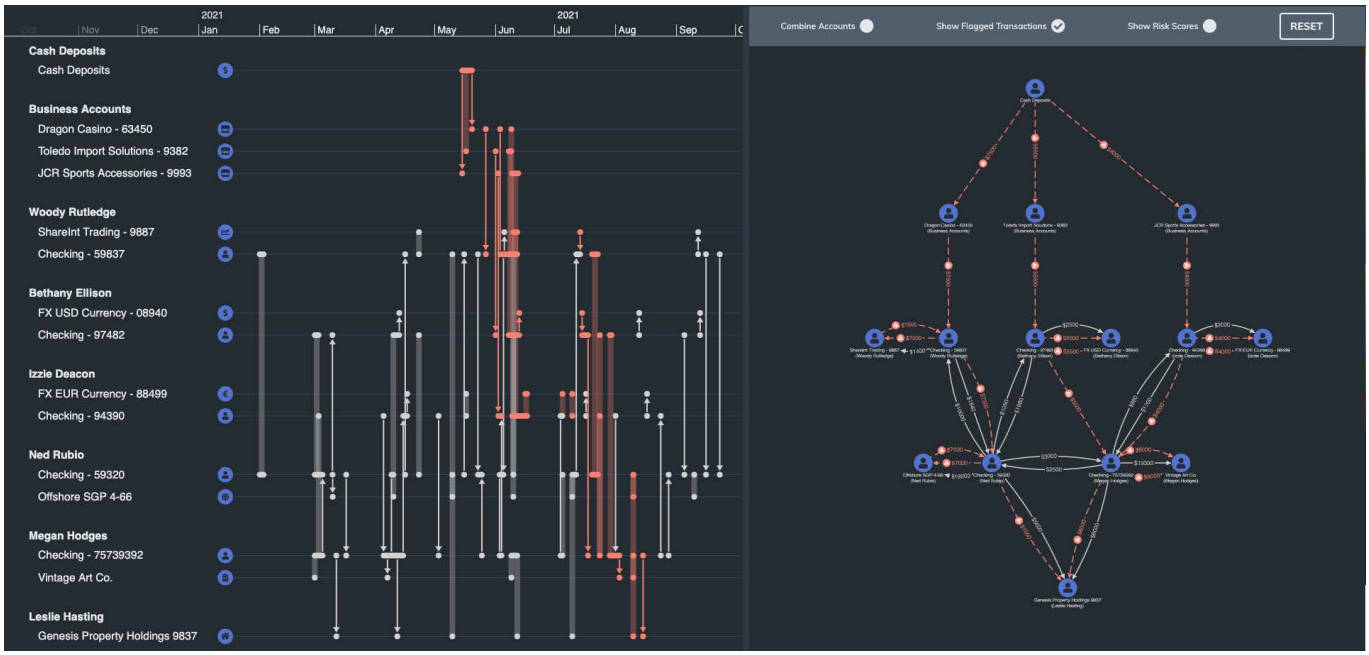
Follow the money

In this scenario, we’ll follow the money through a series of typical money laundering steps. Here we can see a set of accounts and transactions, represented as both a timeline and graph.



The timeline, on the left, shows a set of transactions within a certain timeframe. The graph on the right shows the transactions moving through the accounts. These two views are integrated - so selecting an entity or transaction in the timeline highlights its counterpart in the graph, and vice versa.

We can highlight suspicious transactions, flagged because they’re larger amounts than normal or because the accounts have previously been associated with criminal activity.



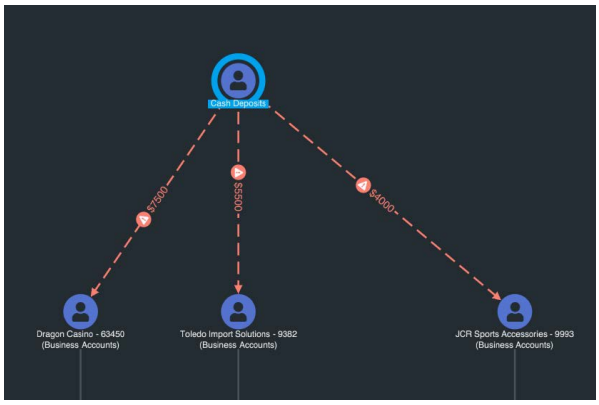
Flagged transactions show as red in both views

The goal of money laundering is to pass the proceeds of crime through enough complex transactions that it's no longer recognisably 'dirty'.

The first stage of this is **placement**, where dirty money is deposited as cash with a front business - often associated with the criminal network.

To see where 'placement' happened, we click the top node in the hierarchy.

The next step is **layering** - where funds pass through an array of accounts to conceal their source.



Dirty money is deposited with three businesses: Dragon Casino, JCR Sports Accessories and Toledo Import Solutions

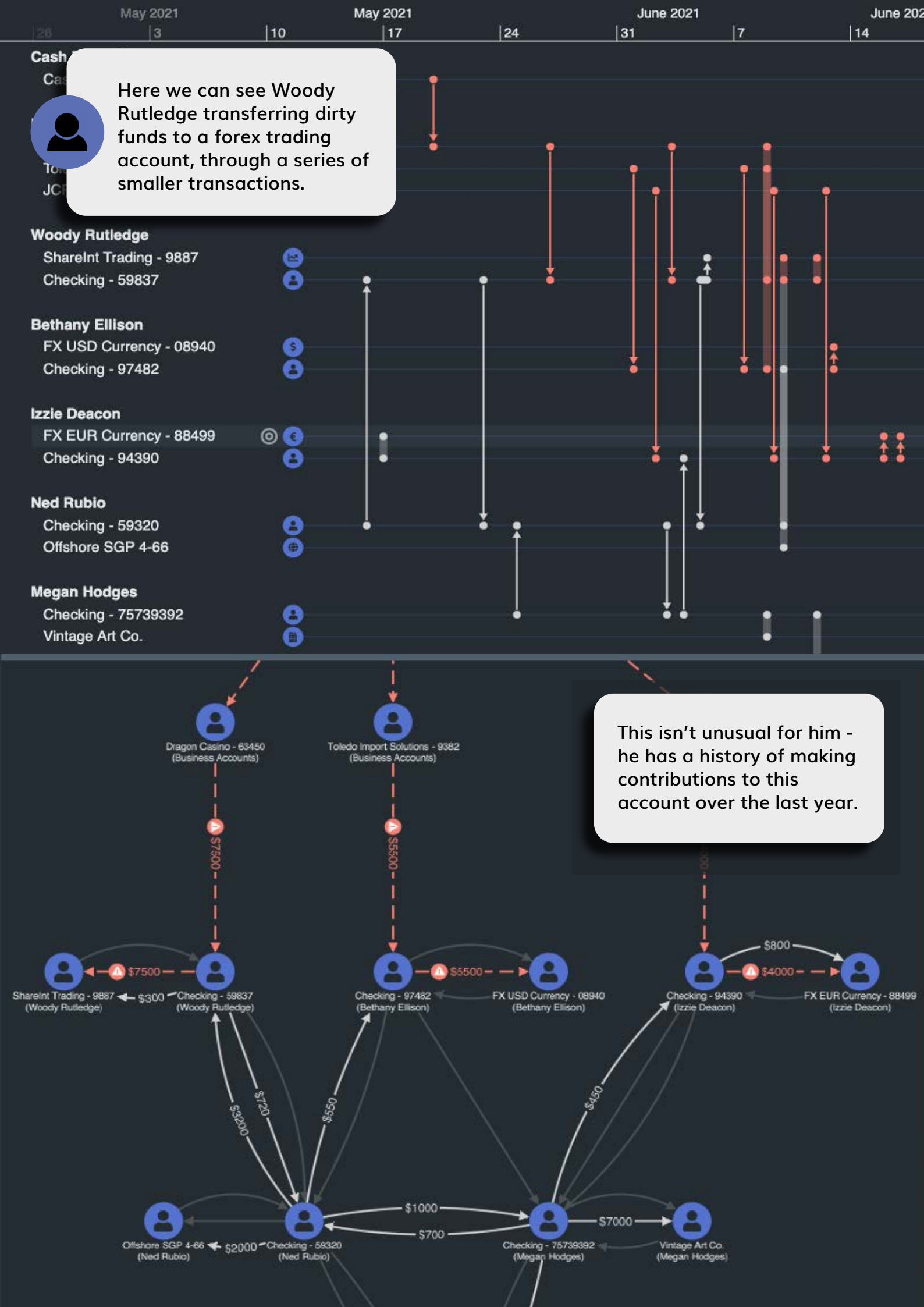
In our graph, transactions are aggregated into single links between nodes, but the timeline shows a more detailed picture. Large and small amounts flow between accounts, both flagged and unflagged. This approach is typical - curating an account history that blurs the line between legitimate and illegitimate transactions.

Custom styling

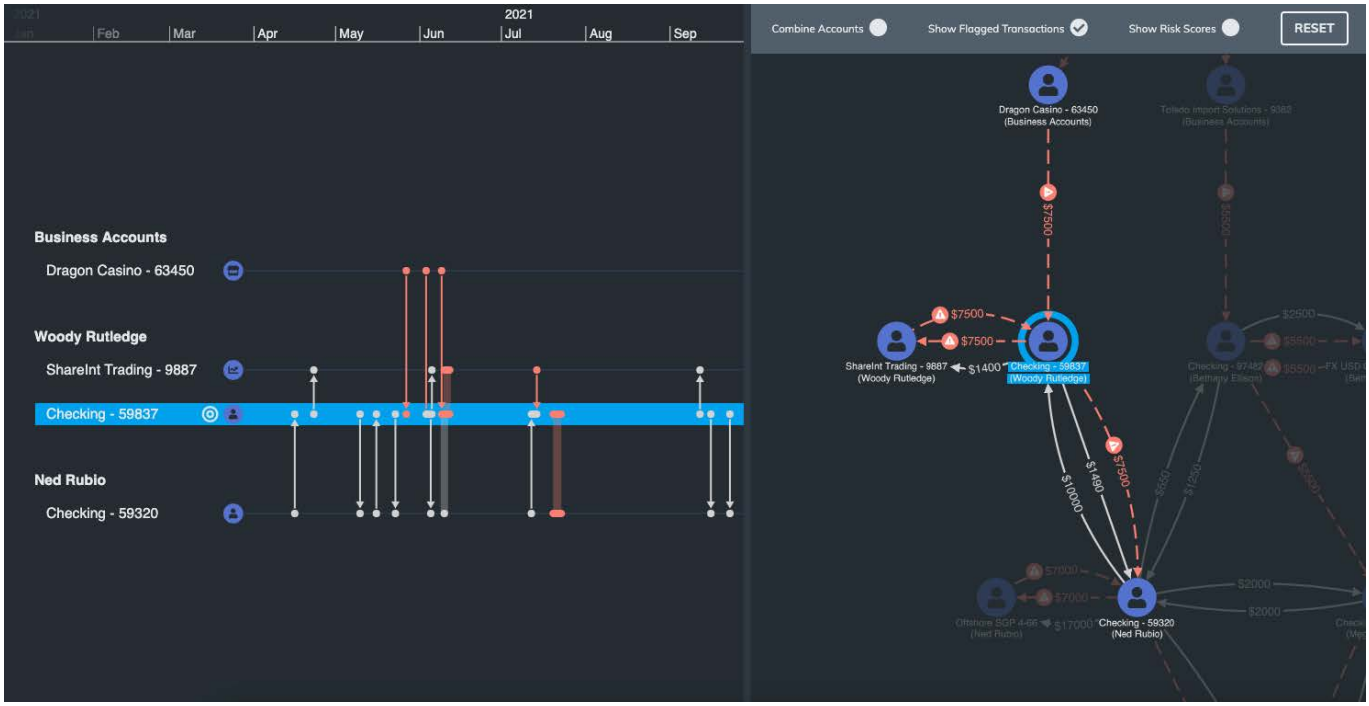
"One size fits all" is usually a compromise. Visual data analysis tools work best when they're customized to your data, your users and the questions they need to answer.

Our SDKs provide limitless flexibility, meaning your visualizations will fit in seamlessly and your data will make instant sense. You can also create a fully-custom user experience, providing users with the analysis options they need in an intuitive and timely way.

Learn about the importance of customizing your data visualization tools.


May 2021
May 2021
June 2021
June 202
26
3
10
17
24
31
7
14
Here we can see Woody Rutledge transferring dirty funds to a forex trading account, through a series of smaller transactions.
Woody Rutledge
ShareInt Trading - 9887
Checking - 59837
Bethany Ellison
FX USD Currency - 08940
Checking - 97482
Izzie Deacon
FX EUR Currency - 88499
Checking - 94390
Ned Rubio
Checking - 59320
Offshore SGP 4-66
Megan Hodges
Checking - 75739392
Vintage Art Co.
Dragon Casino - 63450
(Business Accounts)
Toledo Import Solutions - 9382
(Business Accounts)
$7200
$5500
This isn't unusual for him - he has a history of making contributions to this account over the last year.
$7500
$300
ShareInt Trading - 9887
(Woody Rutledge)
Checking - 59837
(Woody Rutledge)
$5500
Checking - 97482
(Bethany Ellison)
FX USD Currency - 08940
(Bethany Ellison)
$800
$4000
Checking - 94390
(Izzie Deacon)
FX EUR Currency - 88499
(Izzie Deacon)
$3200
$720
$550
$450
$1000
$700
$7000
$2000
Offshore SGP 4-66
(Ned Rubio)
Checking - 59320
(Ned Rubio)
Checking - 75739392
(Megan Hodges)
Vintage Art Co.
(Megan Hodges)

Later, he transfers the funds back into his current account, and then transfers these funds across to Ned Rubio. Again, there is a history of transactions between Woody and Ned. Ned then transfers the funds to an offshore account to further conceal the trail.



The final stage is integration, where dirty money is finally transferred into a legal entity. In this case, it's Genesis Property Holdings. Ned has a history of transferring money to this company, so this isn't unusual. With his carefully-curated 'low risk' profile, this transaction could otherwise seem legitimate.

Thanks to the graph and timeline view, however, we can see that these individual transactions are part of a much larger fraudulent web.

Our software development kits

At Cambridge Intelligence, we build software development kits (SDKs) for visual graph and timeline analysis.

They make it quick and easy to build high-performance visualization tools, ready to deploy into your existing products and applications, anywhere.

Get there faster

Building visual analytics tools from scratch is hard and expensive.

With our SDKs, small teams can build great things and deliver them to users in weeks - saving months or years of effort.

Enjoy the perfect fit

Visual tools built with our SDKs are the perfect fit for any device, browser or data source.

Wherever you need to deploy graph and timeline capability, you can do it with our SDKs.

A trusted partner

We've been the leading provider of graph and timeline technologies for over a decade.

More than 250 customers in 35 countries trust our software, from governments to startups.

About Cambridge Intelligence

From law enforcement to cybersecurity and fraud detection, every day, thousands of analysts around the world rely on our software to 'join the dots' in data and uncover hidden threats.

Hundreds of organizations have already deployed applications built with our toolkits to detect and investigate fraud.

Learn more or register for a free trial on our website: cambridge-intelligence.com/try/

KeyLines

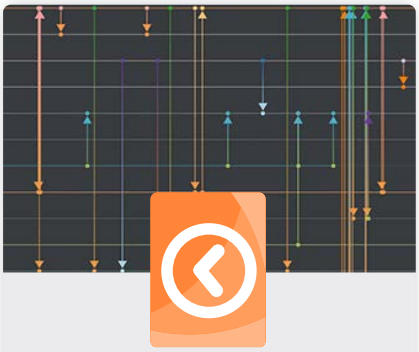
is a graph visualization toolkit for JavaScript developers

Add graph visualizations to your applications that work anywhere, as part of any stack.

ReGraph

is a graph visualization toolkit for React developers

ReGraph's data-driven API makes it quick and easy to add graph visualizations to your React applications.



KronoGraph

is a toolkit for building timelines that drive investigations.

With KronoGraph it's easy to build interactive, scalable timelines to explore evolving relationships and unfolding events.

Cambridge Intelligence

cambridge-intelligence.com USA +1 (775) 842-6665 UK +44 (0)1223 362 000
Cambridge Intelligence Ltd, 6-8 Hills Road, Cambridge, CB2 1JP