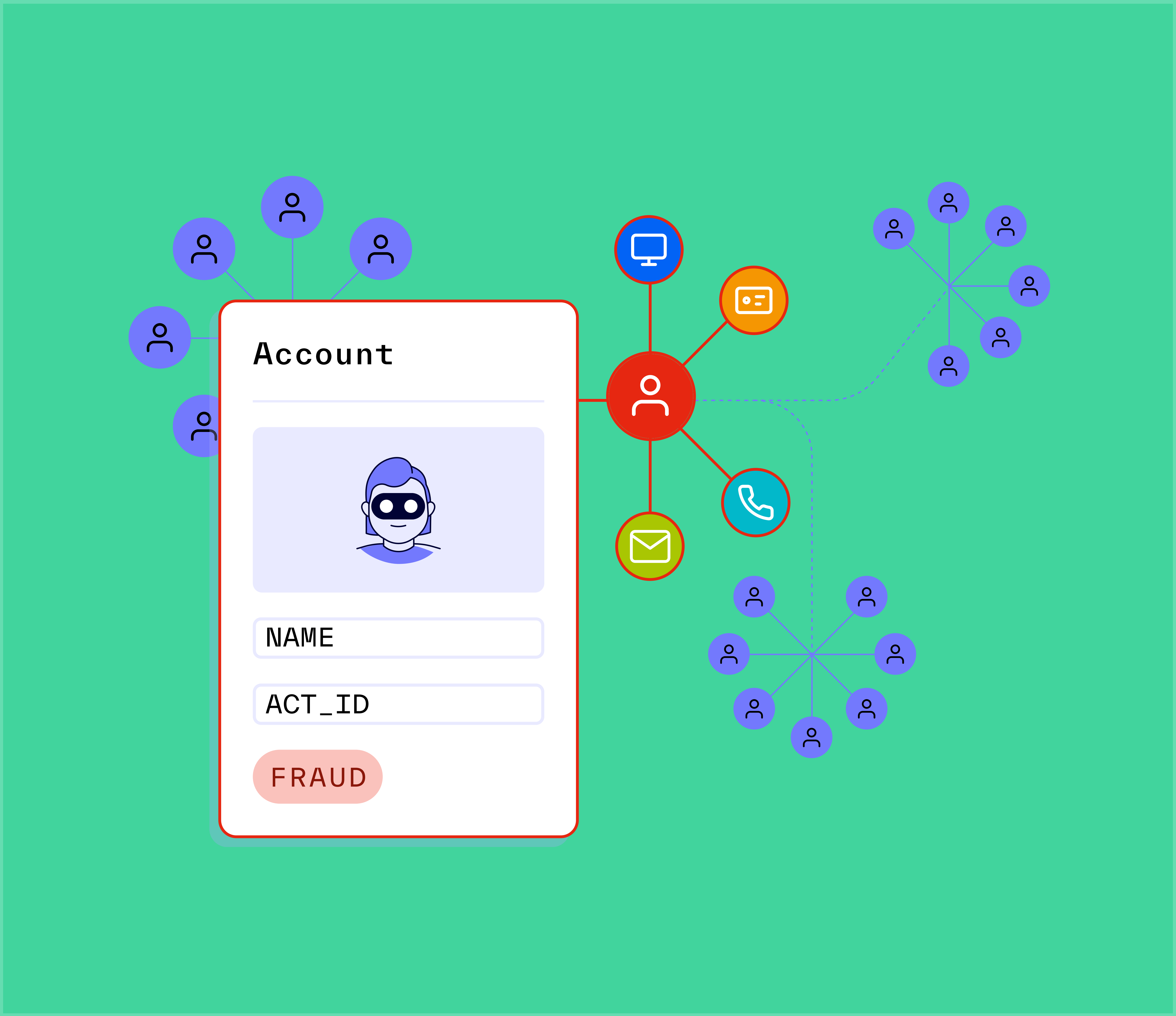
persona

Stop the Revolving Door of Fraudsters With Link Analysis



The good news is your company is growing. The bad news is fraud rings are noticing.

With an increase in large-scale fraud attacks and repeat offenders, you can no longer ignore how some of your initial solutions and workarounds — creating block lists by painstakingly combing through disparate data points, running manual database queries, and even building your own tools to combat bad actors — have become less effective and more time-consuming.

While know your customer (KYC) and know your business (KYB) processes can help you catch less-experienced bad actors, large-scale attacks and fraud rings can only be efficiently and effectively caught through a more holistic and aggregate approach.

Uplevel your fraud-fighting strategies

Many companies concentrate their fraud-fighting efforts during KYC/KYB — for example, adding friction during onboarding or reverifying users when unusual behavior is detected. While this is a good start, it's impossible to see in real time who these fraudsters are linked to on your platform and expose larger fraud rings.

For that, you would need link analysis, a method of analyzing data that allows you to study relationships that aren't visible in raw data, investigate at scale, and stop the revolving door of fraudsters.

If you want to increase your ability to both proactively catch fraud and react faster, this ebook is for you. And as an added bonus, the link analysis tool we'll introduce on page 20, features an intuitive query editor and does not require engineering and product resources! Let's dive in.

Table of contents

What is link analysis? 04

Benefits of link analysis 06

The power of link analysis + KYB/KYC 08

Fortify your fraud-fighting arsenal with link analysis 09

Efficiently and effectively investigate synthetic fraud with Graph 10

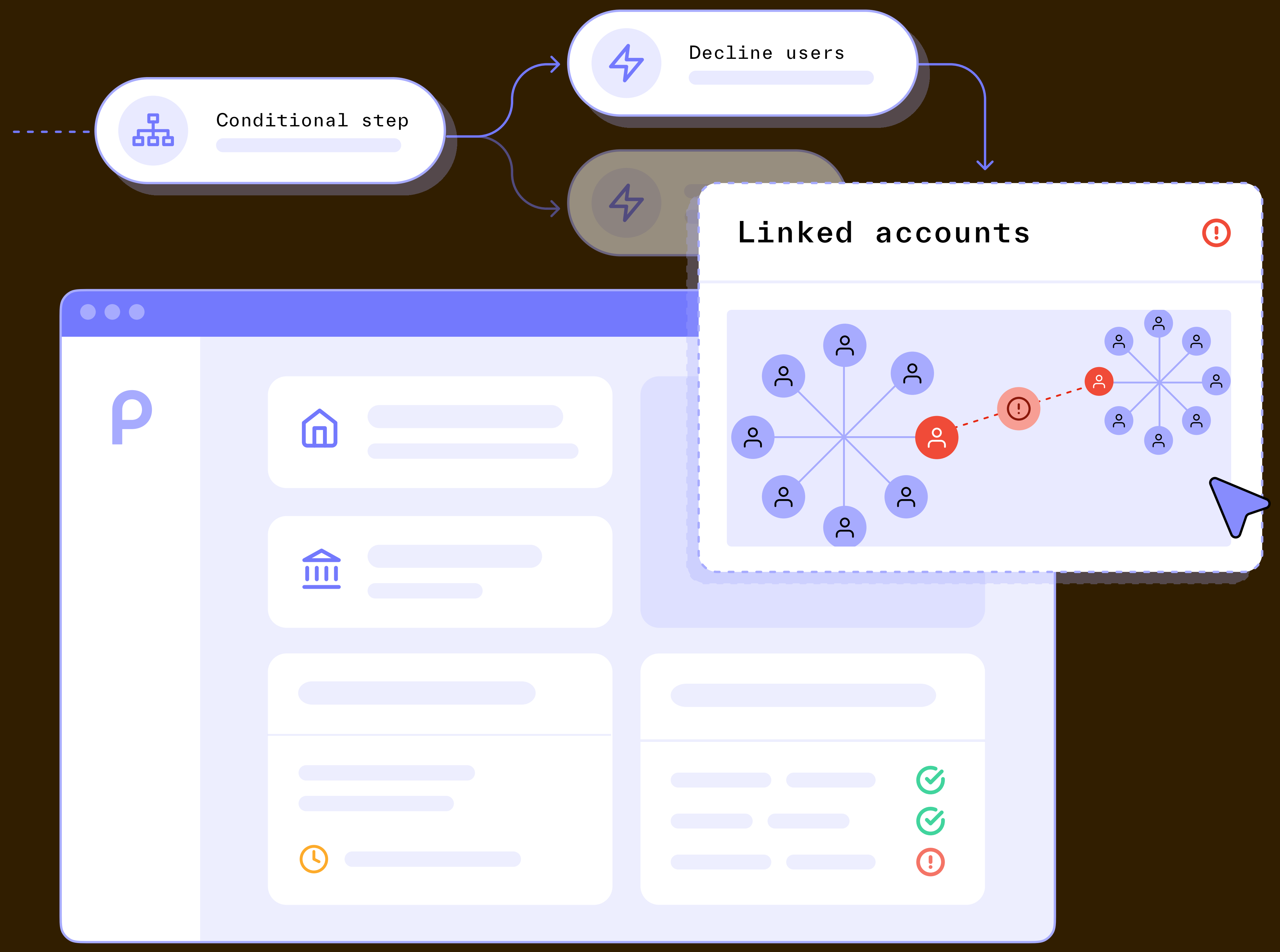
Looking to the future 12

Key takeaways 13

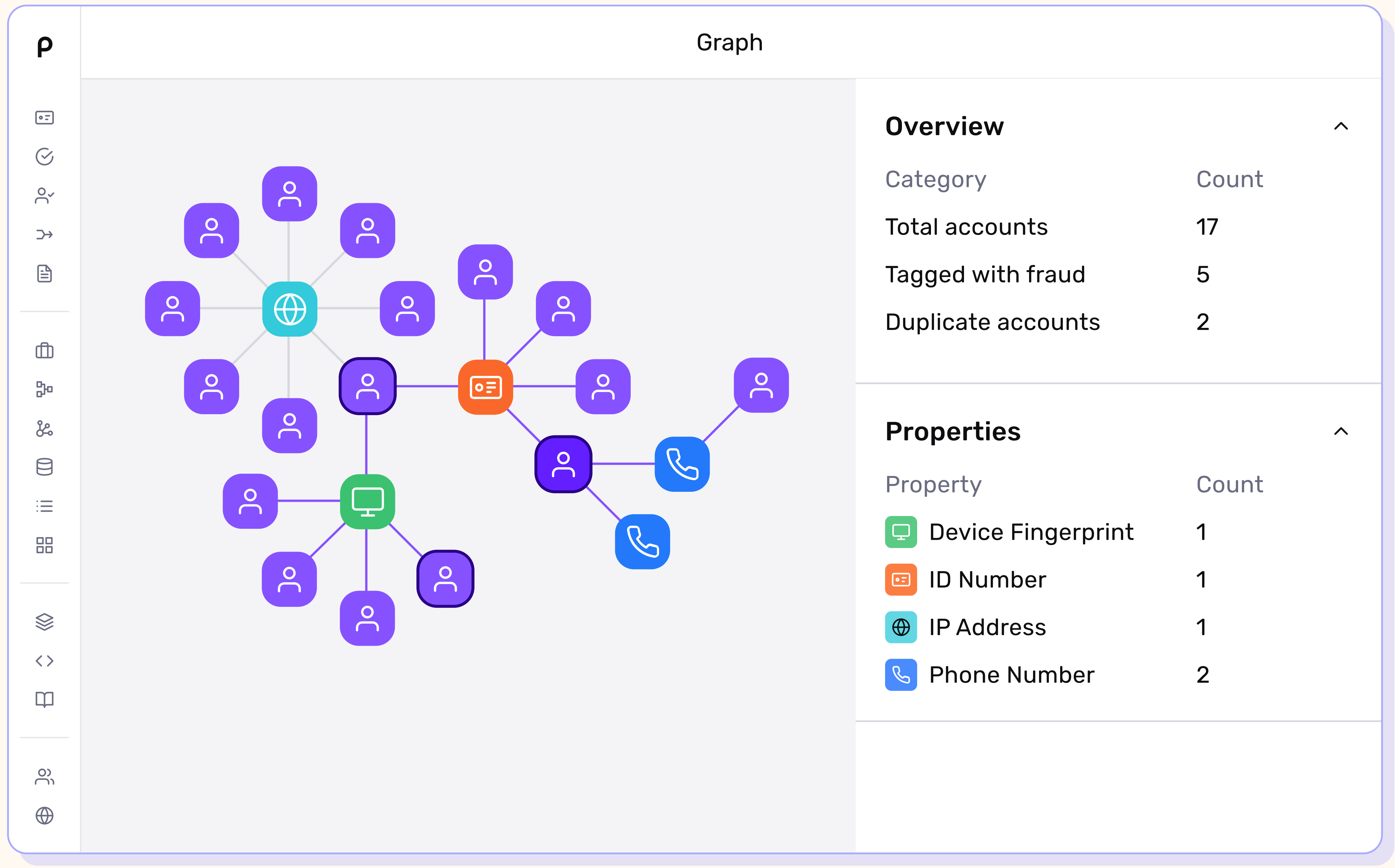
01

What is link analysis?

As mentioned above, link analysis is a method of analyzing data that allows you to study relationships that aren't obvious in raw data, which can help you decipher which of your users may be bad actors. Typically, link analysis starts to make sense as a fraud-fighting tool when your engagement and volume increases.



Advancements in graph database infrastructure — chiefly, the ability to process more graph data and run parallelized graph algorithms — have made it possible to accelerate laborious, error-prone processes and convert data that was once stored in tables to a visual representation of a query like this:



Graph

Overview

Category	Count
Total accounts	17
Tagged with fraud	5
Duplicate accounts	2

Properties

Property	Count
Device Fingerprint	1
ID Number	1
IP Address	1
Phone Number	2

From the above, you can see that each property or signal in the query is represented as an individual node. However, some of the nodes are linked to additional accounts, showing that a single ID number has been used by four accounts, and two of those accounts share properties with 12 additional accounts.

~50%

of fraudulent accounts are linked to 1+ other risky accounts

This intuitive visualization allows for a more thoughtful approach to fraud investigation. At times, something may not seem suspicious by itself, but certain red flags may begin to appear when looking at the information in aggregate.

Which signals does link analysis consider in fraud detection?

Link analysis can consider virtually any signals that a business collects about its users and accounts. Common data points include:

- Names
- Email addresses
- Phone numbers
- Physical addresses
- Payment details
- IP addresses
- Device fingerprints
- Merchants purchased from
- Payment cards/methods
- Billing addresses

Beyond this, link analysis can also consider user activity. For example, a social network using link analysis to understand its members might consider whether accounts share interests or have interacted with a mutual third account, etc.

02

Benefits of link analysis

Stop sleeper accounts before they strike

Save time on manual investigations

Expose deeper connections by looking at connections multiple degrees away

Uncover fraud rings' full breadth

Link analysis has four main purposes. It can be used to:

01 Look for suspicious clusters of linked accounts:
Because network relationships tend to follow patterns, you can use link analysis to identify anomalies in the data or violations of known patterns.

For example, let's say you recently increased your food delivery service's referral bonus from $50 to $300. You then notice hundreds of new courier accounts were created on the same day with the same IP address. Link analysis can plot this activity and show you what else might be linked to this suspicious cluster.

02 Look for new patterns:
Active networks are constantly changing. This means that new patterns can periodically emerge.

For example, a fraudster may attempt to evade detection by changing a single attribute to throw you off — perhaps generating a new device fingerprint or using a clean one. Link analysis can be used to identify these new patterns, enriching what you see on screen and underscoring the importance of a deep bench of signals.

03 Look for accounts linked to a known fraudster:

After your review team has determined that an account is fraudulent, use link analysis to determine whether this is a one-off attempt or if you are dealing with a large-scale fraud attack.

For example, a user account with the IP address “192.158.1.38” was deemed fraudulent. Using link analysis to search for this IP address, you could potentially uncover hundreds of other linked high-risk accounts.

04 Act on entire fraud rings at once:

In response to recent spikes in fraud volume, your review team will want to expose as many fraud rings as possible. To do this, they can run queries with a specific piece of PII, as in the scenario detailed above, and add every account with the matching PII to a block list.

To go a step further in fraud prevention, you can also run cluster searches to uncover accounts sharing an unusual combination of properties. Let’s say you want to query all clusters with at least 5+ linked accounts that share properties (IP address, email, social security number, etc.). Taking the same referral bonus scenario as before, you could go a level deeper by using link analysis to search for all clusters with 5+ linked accounts, uncover multiple fraud rings, and block them all at once.

> “
>
> It’s actually been pretty phenomenal. [Graph] cuts through a lot of those issues, especially quickly identifying if this is a problematic group of individuals or a lone wolf bad actor. We can look for those common threads of IP, device ID, address, phone number, verification documentation, government IDs, things like that, find those common threads, and be able to quickly — without pulling in another team — go and figure out what we’re dealing with.
>
> SIMON FULLERTON, SENIOR MANAGER, TRUST AND SAFETY | Neighbor

You can see how link analysis is a pretty powerful tool for spotting suspicious activity that may be many degrees away from the starting node, and investigating at scale without having to hopscotch across databases and platforms.

03

The power of link analysis + KYB/KYC

While verifying identities as part of your KYC or KYB process can help weed out bad actors, it's not 100% foolproof. Bad actors will continually try to find new ways to infiltrate your business. Bots and other large-scale fraud attacks can pass the verification process or overwhelm your systems with attempts.

By combining link analysis with identity verification (IDV), you can shut down a bad actor who repeatedly commits fraud by visualizing linkages between users and accounts sharing the same risky signals, and use this data as a starting point for investigation. Without link analysis, launching investigations and understanding the scope of a single fraudster's reach is not only time-consuming, but also can pose a huge risk to your business if not dealt with swiftly.

> Linking systems like Graph are so important. We wanted something like this very badly, and we were already using Persona's ID verification processes, so when they showed us the tool, I immediately said, 'Yep, I want that.'
>
> SIMON FULLERTON, SENIOR MANAGER, TRUST AND SAFETY | Neighbor

04

Fortify your fraud-fighting arsenal with link analysis

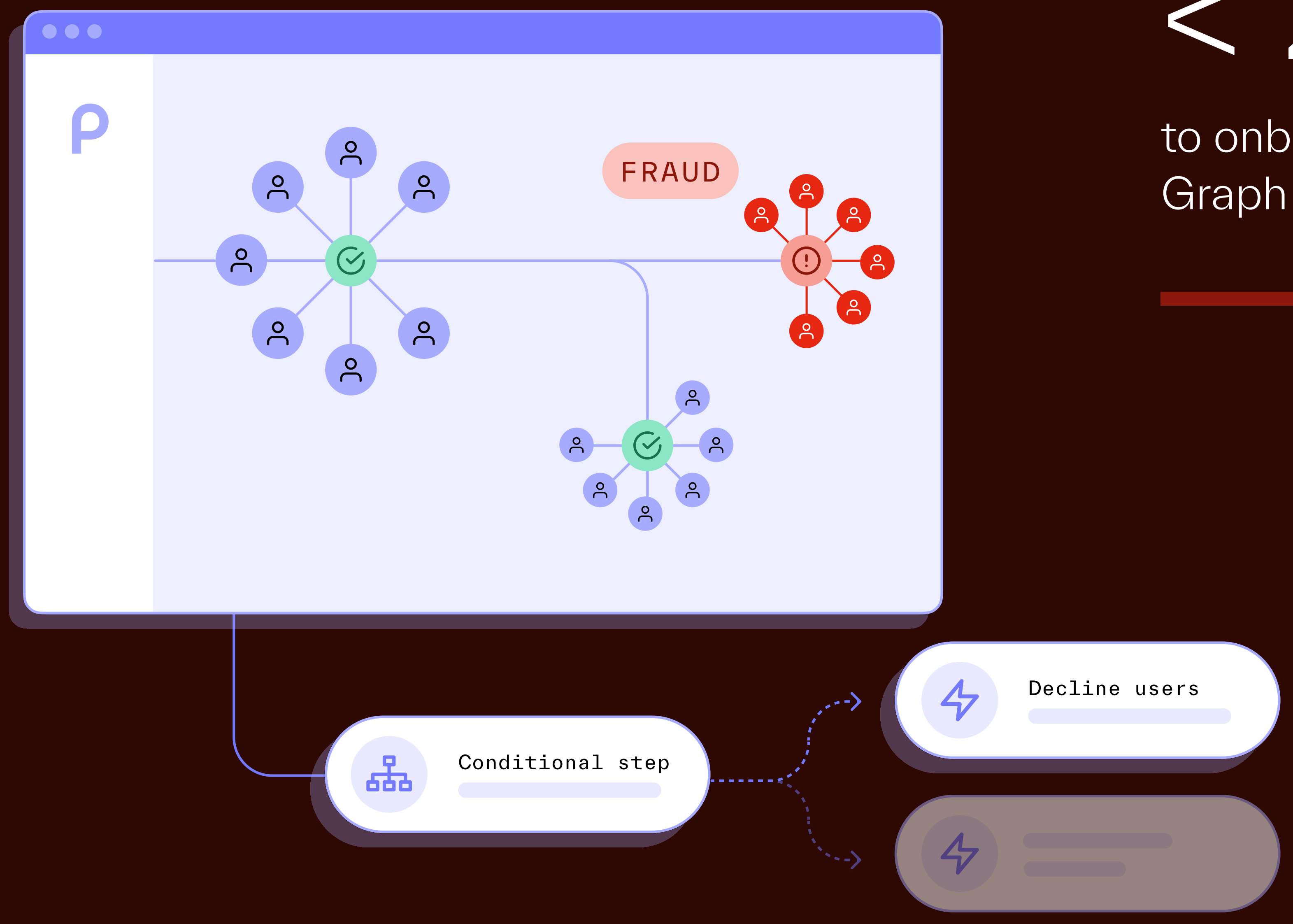
Some fraud is successful because it is extremely sophisticated and hard to detect by machine or human intelligence. The combination of link analysis and other tools such as automated verifications and dynamic workflows can help you catch a lot more fraud, encompassing everything in both columns below:

Identity verification can help you	Link analysis can help you
Prevent an account from being opened with a synthetic ID and stolen bank details	Prevent bots and fraud rings from opening hundreds or thousands of accounts with synthetic IDs and stolen bank details
Prevent account takeover or inconsistent reverification during high-risk moments transactions	Prevent all instances of the same bad actor taking over other accounts
Monitor an individual's activity for suspicious transactions and activity, which may indicate chargeback or other types of fraud	Monitor activity between multiple accounts to identify suspicious transactions, which may suggest a fraud ring engaged in money laundering or widespread fraud
Identify a sanctioned company or individual posing as a legitimate business or person during onboarding	Surface all links to a single sanctioned individual or company

05

Efficiently and effectively investigate synthetic fraud with Graph

Now that you know what link analysis can do, discover how you can onboard Persona’s Graph solution in as little as two days — without tapping product or engineering resources. For many of the fast-growing businesses we work with, synthetic fraud is a critical problem that Graph helps them address with its data visualization and automated decisioning capabilities.



REDUCE TIME TO LAUNCH

< 2 days

to onboard your entire team to Graph and start investigating

As AI technologies become commodities, they become convenient mass weapons for fraudsters to generate deepfakes, voicefakes, and synthetic IDs. Here's one scenario of AI-driven fraud:

Let's say you're a mid-size company that recently increased your referral promotion from $50 to $300. At first, it was easy to identify promo abuse conducted by bad actors trying to use similar email addresses. But later on, you noticed a spike in illicit accounts created with no initially obvious links, except that they were created during the same 24-hour period.

At this point, your review team might turn to one of two common options below:

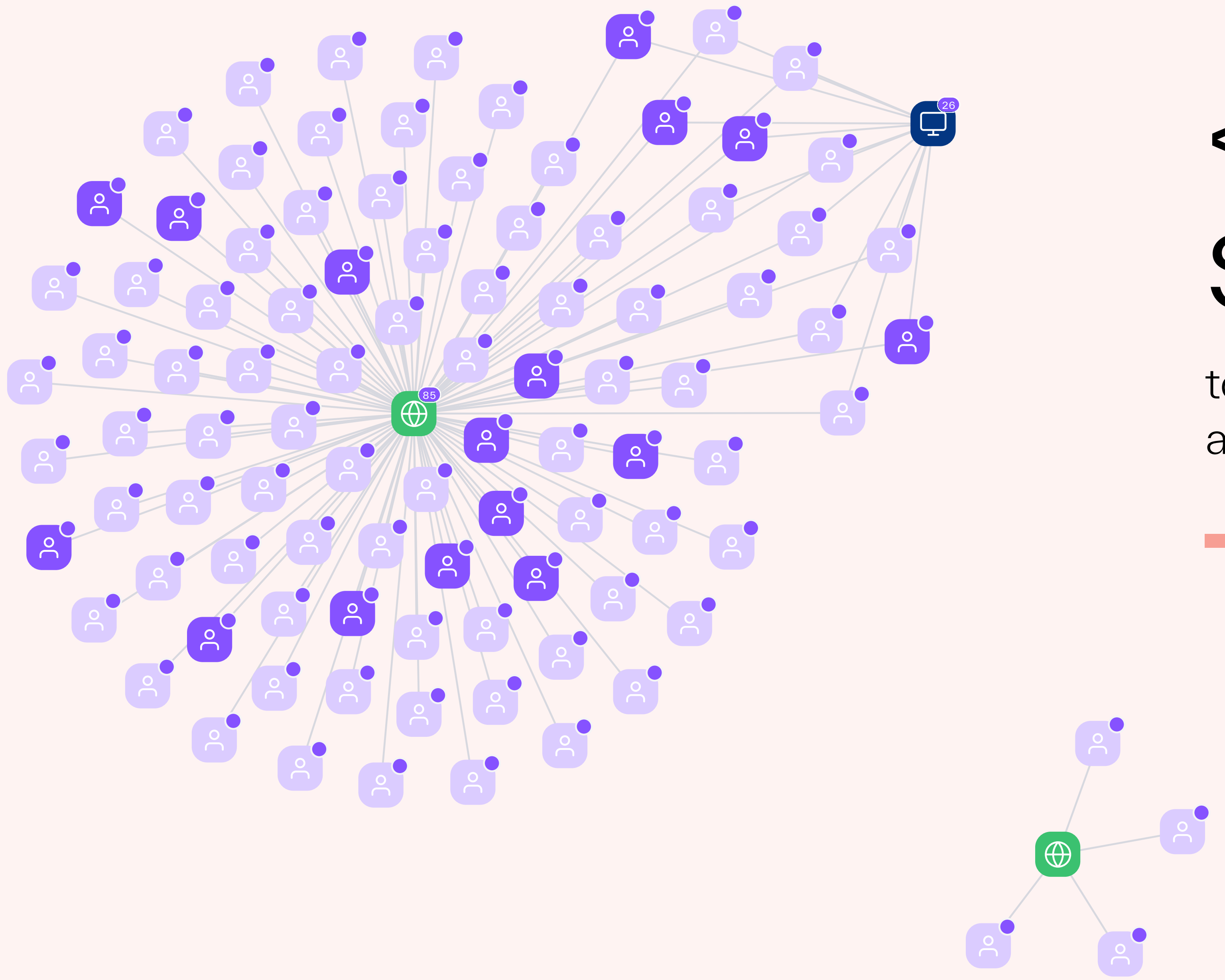
- Manually query your database, which can take several days
- Feed the data from the flagged accounts into an in-house tool built by your product and engineering team, who do not have the bandwidth to maintain it

> "
>
> We relied on our development team to manually query our database to find linked accounts. **This was costly, and it took a long time to complete.**
>
> RENE HAKIKI, EXECUTIVE PRODUCER | nWay

Using either method, you'd only be able to catch fraud retroactively, which would delay your fraud-fighting efforts — ultimately costing your business more money.

By leveraging Graph for investigation, your review team can not only quickly see that many of these accounts were created with synthetic IDs featuring AI-generated faces, but also compare active and passive signals (IP address, transactions, device tokens, and more) and import customer data (hashed bank account details) to see which ones were linked.

The image below is an example of a similarity cluster generated by Graph using data points from identity information collected and verified through Dynamic Flow, our risk response and verification engine. Findings requiring manual review can be automatically sent to Cases, our case management hub. Right in Graph, review teams can also flag and block entire fraud rings, automatically denying entry to any future account sharing attributes with known bad actors.



< 3 seconds

to run complex Graph queries across millions of nodes

06

Looking to the future

There's no silver bullet for fighting fraud — your strongest line of defense blends technology with teamwork: sharing the new types of fraud you are seeing, aligning with internal teams such as product and compliance, and fine-tuning processes such as segmentation and dynamic identity verification.

As graph database infrastructures mature, expect to see more types of data and sophisticated, actionable analytics emerge that can enrich your world view and enable you to make decisions faster. More data may not guarantee better results, but it does enable more possibilities for catching fraud before it happens, preserving the integrity of your platform, and keeping your customers safer.

> “
>
> I've seen a lot of organizations respond to immediate fraud threats tactically and gradually morph into a reactive fraud program. Fraud personnel feverishly update controls which typically lead to results that, quite frankly, create more alerts. They throw more bodies into operations to manage those alerts — it becomes a vicious cycle. There needs to be a greater investment made across the market into strategy versus hiring more investigators. For example, conduct a fraud controls assessment or dedicate full-time resources to proactively analyze data trends that can be actioned more holistically.
>
> BRIAN KILLEN, DIRECTOR | Guidehouse

07

Key takeaways

Move from reactive to proactive fraud fighting

Once fraudsters spot a vulnerability, they'll continue to exploit it until it's fixed. What starts small will always become a larger issue until you take steps to stop it. With Graph, you can spot and stop fraud rings before they get out of control.

You can catch more fraud and easily conduct expert-level investigations without product or engineering resources

You can solve your fraud challenges on your own without burdening product and engineering. It can take as little as two days to onboard your entire team onto Graph and start investigating.

Link analysis with automated decisioning can enable you to stop the revolving door of fraudsters

By visualizing the links between one bad actor or one seemingly random cluster of abnormal activity to others in your database, you can eradicate entire fraud rings and automatically deny entry to any future account sharing attributes with known fraudsters — exponentially increasing your ability to catch fraud *before* it happens.

We’re Persona.

At Persona, we know how important it is for online businesses to understand how their users are related to one another. That’s why we’ve developed Graph, our link analysis solution specifically designed to help you uncover fraud rings by visualizing your customer network.

Graph is just one part of our unified identity platform that gives businesses the building blocks they need to securely collect, verify, manage, and make decisions about individuals’ and businesses’ identities — along with automation and orchestration tools to streamline the entire process from end to end. Founded in 2018, Persona is headquartered in San Francisco and is available in 200+ countries and territories and 20 different languages.

If you’d like to consolidate your data, explore connected users, and stop the revolving door of fraudsters, get in touch.

This ebook is provided “as is”
for informational purposes only
and is not intended as legal advice.