persona

The Fraud Fighter's Guide to Optimizing Your Team and Technology

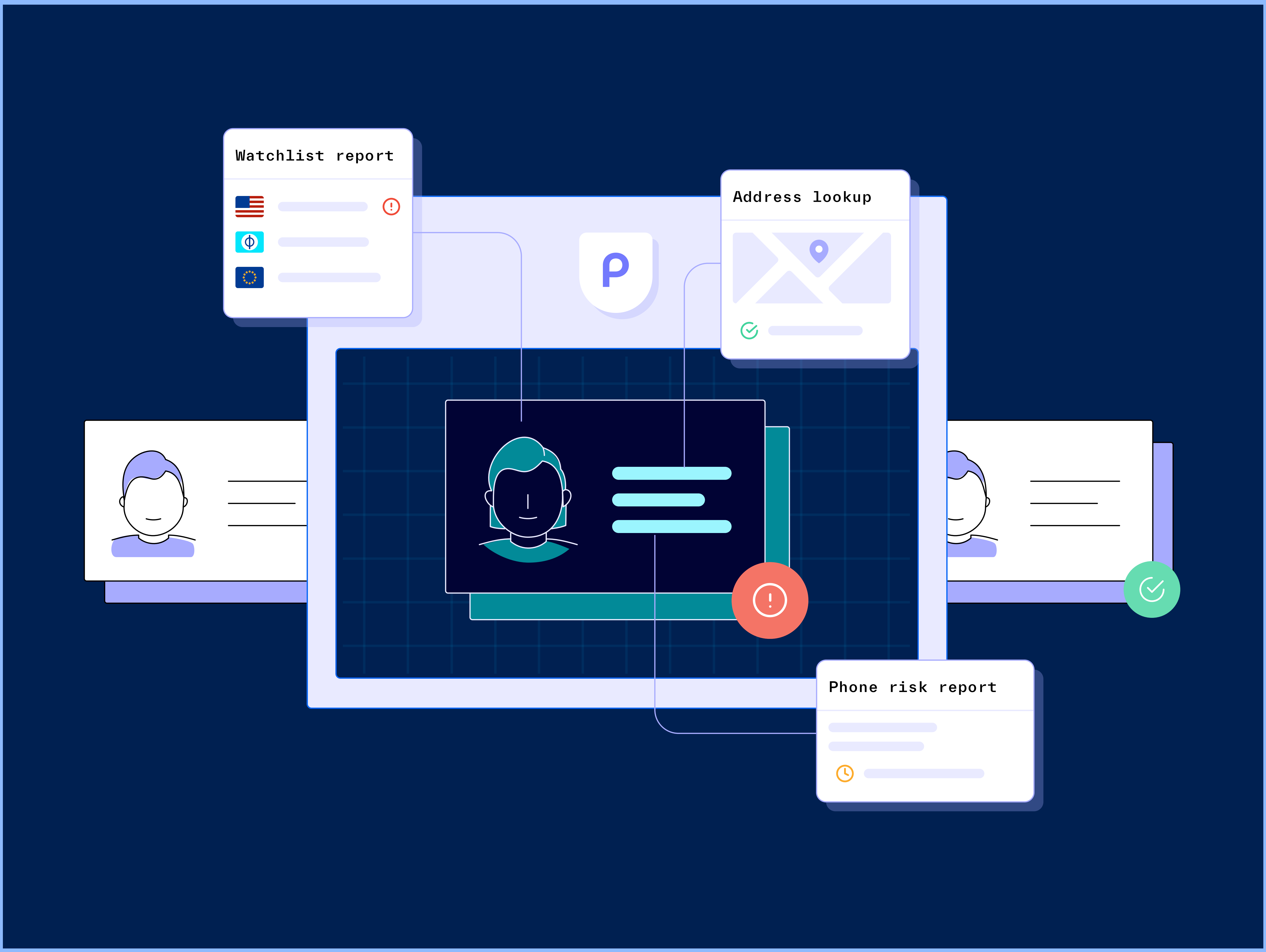

Table of contents

01

Introduction

At least once a year, a moment comes along that allows you to advocate for your team budget. It could be during planning season, when you're starting a new job, moving into a new role, or have a new leader.

Whichever the case, you've thoughtfully presented a reasonable proposal with necessary technology investments that will empower your team to scale and proactively address emerging threats.

Unfortunately, more often than not, a familiar push and pull between the fraud team and the finance team emerges, and before you know it, the higher ups are telling you to stretch your existing budget — or do more with less.

After all, fraud fighting sits on the operational side of any business. At best, it's viewed as a strategic function necessary for building trust, meeting compliance, and preserving revenue. At worst, it's seen as a cost center that needs to be kept as low as possible.

If you feel like your concerns about the pervasiveness of identity fraud and how your organization can better protect your business are well-received but not implemented, you're not alone. In a survey we recently fielded with 500 risk, fraud, and trust and safety professionals, we discovered a near-even split among respondents who shared that their concerns are dealt with immediately versus those who are ignored altogether or not taken seriously until a problem occurs.

Do you feel like your concerns are well-received or ignored by your organization?

54%

MY CONCERNS ARE WELL-RECEIVED AND DEALT WITH PROACTIVELY

41%

MY CONCERNS ARE WELL-RECEIVED BUT AREN'T DEALT WITH UNTIL A PROBLEM OCCURS

6%

MY CONCERNS ARE IGNORED ALTOGETHER

In this guide, we offer advice you can use to better advocate for your team and resources, whether your budget is decreasing, staying the same, or increasing.

02

Spoiler alert — there is no “easy” button

Advice for all three of the budget scenarios we discuss will involve some level of investment in technology, whether it’s recalibrating your existing stack or evaluating new solutions.

However, this doesn’t mean you can buy your way out of a problem, as there’s no silver bullet to fighting fraud. Before diving in, let’s debunk a few myths:

Myth #1: Buying a solution guarantees improvement

Just because you buy the same solution that everyone else is using doesn't mean your organization will automatically see improvements on the fraud front. Your fraud needs depend on factors that are unique to you: your industry, customers, products and solutions, maturity level, and risk exposure.

Even if you decide to go with a solution that comes highly recommended by your peers, you can't just set it and forget it. The best solutions will require some level of regular fine-tuning, because after all, fraudsters are doing the same thing. What works today to keep bad actors out will not work tomorrow.

Myth #2: Working with a consultant or solutions provider means you can be less hands-on in picking a solution

Sure, a consultant (or other solutions provider) can help you identify the tools and technology that make the most sense for your organization. However, for them to be most efficient and effective, there are certain conversations that need to happen first — conversations around your business's challenges, goals, needs, and what matters most to you.

A consultant can't make recommendations about streamlining your processes, for example, without first knowing how your team currently uses manual review and how open you might be to automation.

Before engaging with any third party, it's important to document your internal requirements and thoughts on customer support, what you'd like to see in a product road map, data privacy, and compliance, as well as the scope of your engagement. Otherwise, you may end up wasting time, effort, and the budget you're trying to maximize.

The reality

With this in mind, it's important to resist the temptation to buy a platform that claims to address all of your needs or engage a third-party without doing your own due diligence. Instead of buying a bloated system that includes features you'll pay for but never use, look for a solution (or solutions) that provides building blocks that you can pick and choose from in order to build an anti-fraud program that truly reflects your needs.

03

Key considerations for evaluating anti-fraud solutions

As you evaluate different anti-fraud tools, have these questions handy:

Support

Who do you contact for support, technical or otherwise? How do you contact them — by email, phone, Slack, JIRA, or some other system? What is the average turnaround time for tickets? What resources and documentation exist for your developers and other team members to reference?

You want to be sure that once you purchase a solution, you won't be left to fend for yourself during implementation or as issues arise.

Automated vs. manual

What is the solution provider’s approach to balancing automation with manual review? Does it have relevant case studies to share on how it helped decrease the need for manual review through automation? Is training included with implementation?

The tooling your team will find most useful should fit neatly into your existing processes and even improve them — and offer the right amount of support for implementation and training. In short, work with vendors that make your life easier, not harder.

Product road map

Which functions or features has the solution provider recently shipped? Which releases or updates do they have in their pipeline? Do they accept suggestions from customers?

A vague road map may indicate a stagnant product failing to adapt to new fraud challenges. You want to see a steady cadence of new, customer-centric features that suggest the potential for a long-term partnership.

Data privacy and compliance

What do the solution provider’s security and privacy policies look like? Do they comply with the laws, regulations, and industry standards that matter to you? Will they store personally identifiable information (PII) for you so you can focus more on your business, knowing that user data is well-protected?

Having this information on hand will help you trim down your list of potential providers and get buy-in from cross-functional leaders.

SCENARIO 1

A decreased budget — lean on your vendors to fill in the gaps

You have to do more with less — you've heard this before, right? While it's far from ideal, this is your chance to clearly state what your team can still do, but also what it can no longer accommodate. For that latter bucket, here are suggestions for filling the gaps while maintaining team morale and serving the business as they've come to expect. Don't be afraid to significantly rethink your processes.

Explore or further embrace automation

For most fraud teams, headcount tends to be the largest line item in the budget. If you have to make do with a smaller team, find ways to automate repetitive or tedious tasks. This can enable your team members to focus on the work that provides the most value to your organization and gives you the budgetary flexibility to shift resources.

Not sure where to start? Ask your team which tasks they would automate if given the opportunity. That way, you won't just be saving on time and costs — you'll also be demonstrating to your team that you're working to make their jobs easier.

Deploy progressive risk segmentation

Do you treat all of your customers or users as though they pose the same level of fraud risk to your organization? Doing so could be costing you money. Certain forms of identity verification, for example, may be highly effective — but may also be more expensive to implement and leverage than others, and introduce friction that can impact conversion rates.

Progressive risk segmentation allows you to automatically tailor the verification flow to each user based on how much risk you assess in real time. This can help you minimize friction for low-risk customers and free up budget to deploy elsewhere — without compromising your anti-fraud strategy.

Consolidate your tech stack

Fighting fraud typically requires multiple solutions, but if you're buying solutions from multiple vendors, you could be inadvertently paying for overlapping features. Many vendors offer favorable pricing to customers who purchase multiple solutions through them, and may even incentivize migrating away from their competitors.

Where possible, consider consolidating providers. Start by ranking your solutions by how often your team uses them or how much ROI they provide and work from the bottom up, cutting the least-used and lowest ROI solution or vendor.

Ask vendors for support

Be open about the budgetary situation you're in. Your vendors know that if they're going to keep you as a customer, they need to provide you with more value. Ask how you can reduce spend with minimal impact to the business — whether that means leveraging new features, gaining beta access to a product prior to its official launch, or something else. This has become a routine conversation for many service providers due to recent market conditions, and most vendors will have remedies to offer you.

Be clear about the trade-off

Here's where metrics come into play. Show your higher-ups how much fraud your team has caught and year-over-year trends in how your team has successfully scaled operations with the tech stack you currently have in place. The ROI will be clear. With a smaller budget, project how your team's ability to deter, detect, and deny fraud may change for the worse. The more up front and data-driven you are, the more likely it may be that new budgetary conversations can be had if your projections come true.

SCENARIO 2

A flat budget — measure, iterate, repeat

A flat budget may not be what you and your team were hoping for, but it's also not the worst that could have happened. You can still find ways to better position your team against increasing fraud threats by fine-tuning your processes to free up budget that you can deploy elsewhere.

Consider your metrics

Before making any changes to the way your team operates, consider the data. Where are you starting from and how might any changes you make affect the KPIs that matter most to your team — for better or worse? If costs have risen while your budget has stayed flat, what impact will inflation have on your team's ability to reach their targets? Quantify these effects and communicate them to your leadership team so they know the real trade-off that will come with the budget you've been given.

Understand points of vulnerability and inefficiency

In any multi-step process, there are going to be areas where the process breaks down or doesn't unfold exactly as you'd expect. Identifying and addressing these points of leakage allows your team to become more efficient.

Break down the operational process from the moment an alert is generated until the moment it's resolved. Note any inefficiencies along the way and consider possible solutions for each that you can bring to your vendors to address. You may discover new ways of collaborating that alleviate your team of a burden they had previously accepted and come at no extra cost to you. Win-win.

Think critically about your tools

Is your team regularly “hacking” your existing tools or software to get them to work properly? That means those tools are falling short of expectations and adding friction to your processes. Collaborate with your vendor to remove this friction or consider replacements that may better meet your needs and budget.

Identify key areas of automation

As you analyze your processes, you’ll likely uncover new opportunities for automation. Common test cases for automation, even among enterprise companies, center on data consolidation and extraction. Ask your vendors how they can support your automation needs, how quickly they can implement them, and what results they can measure.

Even small wins can add up significantly over time. If your team averages one verification every five minutes, that’s 12 verifications in an hour. Shaving just one minute off of each verification could translate into an additional three verifications each hour, or an additional 27 over the course of a nine-hour work day.

Measure outcomes and iterate

Periodically return to the metrics that matter to your team and determine whether the changes you have implemented have had the expected effects. If so, consider whether those same changes can be implemented elsewhere in your fraud processes. If not, consider what other changes might move the needle instead.

SCENARIO 3

A growing budget — reward your team with new resources

Congratulations! A growing budget means you can further reduce operational friction and even increase your ability to proactively catch fraudsters. Here's how you can make the most of those additional funds.

Listen to your team

Have ideas on where to allocate your budget but want to ensure they'll be useful for your team? Ask them what they would do with a dream budget and identify what they find tedious or unrewarding. With the right new tool or increased support for automation through an existing vendor, you can alleviate your team of certain tasks they find burdensome. It'll be a huge win for you to share metrics on how many more cases they were able to close per week and greater ROI for your investments.

Bring in new data sources

When it comes to combating fraud, the intelligence at your fingertips matters. The more information you can reference or query, the more confident you can be in the conclusions your team draws during an investigation, and the more opportunities you may have to identify fraud. For example, are there new reports that could help your team make more informed decisions? Phone risk reports, email risk reports, address lookups, and more can all enrich your team's understanding of a user or incident and may deserve a portion of your enhanced budget.

Grow your team

If your team has consistently faced increasing demands each year, hiring more team members can be a good idea. But it's important to scale your team responsibly. After all, the budget gods can be fickle: They giveth, but they also taketh away. If you're aggressive in growing your team this year, and next year your budget decreases, that could lead to many difficult conversations as you right-size your workforce. So, hire when it makes sense — for example, bring on a new team member with experience or expertise that your team currently lacks — but don't eschew automation and other solutions that might be better in the long term.

Go on the offensive

Fighting fraud often feels like playing a game of whack-a-mole. Bad actors rarely do you the courtesy of popping up one at a time, making it challenging to shift from reactive to proactive fraud mitigation. While there is no way to completely prevent fraud from happening, there are ways to shift from being mostly reactive to balancing proactive and reactive measures.

Once you've got a comprehensive defense in place — a well-resourced team and documented processes for fine-tuning your fraud tech stack and workflows — it's possible to go on the offensive and proactively find and remove fraudsters on your platform before they cause any damage. Consider allocating a portion of your budget to tools that empower you to do this.

Through link analysis, for example, you can find accounts that share suspicious details — IP addresses, device or browser fingerprints, physical addresses, payment details, etc. — which might indicate a fraud ring — and quickly move to shut them down.

07

Success stories

At Persona, we are privileged to work with many of the world's leading companies to help them deter, detect, and deny fraudsters. Read how three of our customers protect and grow their business by leveraging the building blocks they need from our comprehensive identity platform.

> “
>
> Persona was such a drastic improvement over waiting for days and not knowing when the verification would come back. We always had to worry about this, and Persona entirely removed that pain. We are now in control.

INDERPAL SINGH, GENERAL MANAGER OF TRANSFERS | AngelList

AngelList consolidates Know Your Customer (KYC) process with Persona, paving the way for further growth.

AngelList is the leading platform for investing in world-changing startups. They have users around the world and offer multiple services that require different levels of verification.

Problem

AngelList was using multiple vendors to verify the identities of investors, buyers, and sellers on their liquidity platform. This process was expensive and highly manual, as the vendors didn't connect with each other. As a result, AngelList's operations team was spending unnecessary time managing various aspects of the verification process.

Solution

AngelList found a one-stop solution and partner for all of their current and future verification needs in Persona.

Read the full case study here.

AngelList ultimately chose Persona for the following reasons:

01 Comprehensiveness and customization

When they saw that Persona offers a wide range of verification options and would allow them to serve different flows to different users depending on their use case, they knew it would be a game-changer.

02 Collaboration and dedicated support

With Persona, AngelList gets one highly responsive, dedicated account team — and a joint Slack channel they can use to discuss questions and issues.

03 Fast ID verification

Persona's speed was especially pronounced compared to the vendor that AngelList's transfers team was previously using to run watchlist reports, which would take days.

> “
>
> Everything's in one place with Persona. It's much simpler and streamlines everything. I feel confident that Persona will be able to support us as we continue to scale our business and serve more founders and investors.
>
> JESS TOY, PRODUCT LEAD | AngelList

Empower builds a modern banking experience with automated account recovery

Empower's mobile-first personal finance app offers mobile banking accounts with competitive rewards and a smart financial assistant.

Problem

Prior to partnering with Persona, Empower customers who were locked out of their accounts and did not have their phone on hand were required to email their personal information to the Empower team for manual review. This was an incredibly cumbersome account recovery process for both parties.

Solution

With Persona, Empower fully automated their account recovery process, reducing the need for manual review and increasing the speed of account recovery.

Read the full case study here.

Empower selected Persona for the following key reasons:

01 Data security with a fully automated solution

Unlike many other solutions, Persona's identity verification solution is fully automated, limiting access to customer data and keeping it within Empower's organization.

02 A speedy and seamless account recovery process

Persona's platform allowed new customers to complete their identity verification quickly — via web or mobile — and obtain their results instantaneously instead of waiting hours or days, providing a quick and seamless account recovery experience.

03 No engineering resources required

With Persona's hosted identity verification flow, Empower was able to get up and running without any involvement from engineering or design, freeing up valuable resources they directed toward their core business.

> “
>
> Persona's combination of document verification and live facial comparison ensures a speedy, automated, and highly secure account recovery experience for our customers.
>
> MAC MUIR, OPERATIONS | Empower

nWay decreases chargebacks by 80% and proactively blocks linked accounts with Persona Graph and KYC solutions

nWay is a game developer and publisher whose goal is to create console-quality multiplayer games for both web and mobile. It launched the nWayPlay Marketplace, where users can purchase non-fungible token (NFT) packs, trade individual NFTs with other users, earn NFTs by playing games, and more.

Problem

nWay's fraud investigation process was manual and ill-equipped to pinpoint and fight coordinated fraud attacks. While KYC can help weed out bad actors, it's not 100% foolproof. nWay's main challenge was combating bots and other large-scale fraud attacks where the same risky signals (IP address, device finger-print) were showing up across a group of accounts. These fraud rings were not only time-consuming to catch, but also posed a huge risk to the business if they were not dealt with swiftly.

Solution

nWay discovered the power of link analysis in Persona's fraud investigation tool, Graph.

Read the full case study here.

The reasons nWay chose Persona and Graph include:

01 Speed and automation

With Graph, nWay was able to find and ban fraudsters faster than their previous manual processes allowed.

02 Multiple degrees of separation

nWay found value in Graph's ability to surface risky connections — even those multiple degrees away — between user accounts.

03 Ease of use

nWay appreciated that Graph could not only give them more visibility into the reach of fraud rings, but also equip their compliance team to handle investigations on their own using the configurable, no-code query editor.

> “
>
> The biggest advantage of Persona's Graph tool is that we can proactively block fraud incidents before they happen with automated decisioning. So we're going from more reactive to proactive, and from a compliance perspective, that's a home run.
>
> DAVID KIM, COMPLIANCE PROGRAM MANAGER | nWay

08

No matter your budget, we're here to help

At Persona, we understand how your budget affects your team's ability to fight fraud — and how frustrating it can be when your team isn't given the resources you believe it needs or deserves. The good news? With the right tools and technologies in place, it's possible to:

- Free up budget that can be deployed elsewhere
- Move the metrics that matter most to your organization
- Streamline your processes, reduce friction, and boost your team's efficiency
- Become more proactive in your fight against fraud

To learn more about how Persona can help you meet your KPIs while getting the most out of your budget, contact us and we'll be happy to learn more about your challenges, show you a demo, or share additional resources.

Our solutions include:

- Customizable identity verification
- Global issuing and authoritative verification sources
- Passive behavioral and device-based risk signals
- Supplemental watchlist and risk reports
- Progressive risk segmentation
- Automated workflows
- Link analysis
- Case management
- Data privacy and PII storage
- Modular permissions and access control

Additional resources

Streamline your identity verification processes with a unified identity platform

Read more →

Get the best out of both worlds: How thoughtful manual review can enhance your automations

Read more →

Linked fraudulent accounts: A threat and an opportunity

Read more →

3 tops for managing risk without sacrificing user experience

Read more →

5 questions fraud leaders ask about synthetic fraud

Read more →

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

persona