

How do you swiftly and effectively respond to rapidly emerging fraud threats?

OUTSEER

The challenge:

The evolution of digital financial services and payment options exposes weaknesses in fraud prevention



As digital financial services continue to evolve in response to consumer demands, the pressure's mounting to roll out new digital offerings as quickly as possible. Yet every new service creates another opportunity for fraud.

It's increasingly difficult to stay ahead of new fraud vectors when you can only devote so much time to researching these threats. And point solutions do little to help matters because their field of view is limited to one narrow use case or data signal. Worse yet, many of these tools actively inhibit your ability to share vital data across fraud models and your organization.

For example, you may know a customer's valid device ID from login, but you can't use this data to verify their identity when they make a digital payment. Or, you may have identified fraudulent devices in one system, but can't rely on this intelligence to stop criminals when they make changes to account details. Data sets are limited to what you collect by yourself—with the aperture closing even further for each isolated use case, deployment environment, or channel.

This means you can't make decisions with the speed and accuracy you would like. More fraud gets through as a result, prompting customers, regulators, and stakeholders to ask how you could let it happen.

But when you expand your relationship with Outseer, you'll utilize superior data science to address fraud across key customer touchpoints.

Here's how you'll make it possible...



Leverage insights from the world's largest financial institutions

It takes considerable time and energy to keep pace with the evolving fraud landscape, not to mention the best practices for protecting both your organization and its customers.

With Outseer, you can expand your perspective to defend against the latest fraud vectors being observed by other organizations. Partnering with our professionals, you'll manage fraud relative to peer benchmarks and utilize consortium data from the world's largest, highest-threat environments.

And you'll be able to engage with our customer success team, data scientists, and fraud advisory services professionals from initial project planning and data mapping to establishing the policies you apply to our risk engine to support your objectives.

When you support your fraud prevention efforts with models trained on billions of transactions at the largest financial institutions in the world, you'll keep your organization one step ahead of its adversaries.

Outseer's **vast expertise in digital banking fraud** was built by working with thousands of global organizations over the past 20 years.

Protect your institution with the market's highest-performing fraud prevention

It's critical to use the best fraud models possible—and then fuel those models with the richest data available.

With Outseer, you'll deploy a sustainable and evolving model that's been designed by leading data scientists with deep industry and fraud expertise. You can then feed that model with fraud data that's enriched by both first- and third-party sources, bringing in signals from around the globe.

Finally, you'll be able to deploy this model—and tune it to your specific needs—in a technology platform designed for banking-grade, high-availability, high-throughput, real-time decisions.

With the confidence that you're using a superior model and best available data, you'll separate legitimate and fraudulent transactions with greater accuracy—and do so in time to take the proper action.



Our **data science** is fueled by an ever-expanding Global Data Network consortium drawn from billions of transactions across clients, partners, and third-party data providers.

Drive long-term value with future-proofed deployment options

Every organization needs to align solution deployments with its overall technology strategy, especially since these strategies are constantly evolving.

With Outseer, you can select the most appropriate deployment option for your fraud solution for each region and online channel in which you do business. For example, you can work with the Fraud Manager implementation support team to help you align with your organization's cloud mandates.

Alternatively, you can utilize our on-premise option—without changing any underlying capabilities—knowing you'll have support for any cloud if and when you decide to migrate. What's more, you can support desktop web, mobile web, and mobile app channels.

With support for both cloud and on-premise options built on the same underlying capabilities—not to mention a partner that's expanding the product to meet today's and tomorrow's needs—you can accelerate the introduction of new payment options with greater control and confidence.

Outseer offers **flexible deployment options** that are guided by experts and based on a common set of capabilities.



Utilize superior data science to address fraud across key customer touchpoints

The push for new payment options creates new opportunities for fraud—and exposes you to threat vectors point solutions can do little to counter.

But when you continue your partnership with Outseer, you'll utilize superior data science to address fraud across key customer touchpoints.

This way, you'll be able to:



Stay out in front of evolving threat vectors



Identify fraudulent transactions more accurately



Release new payment options faster



To learn more, please <u>contact us today</u>.

