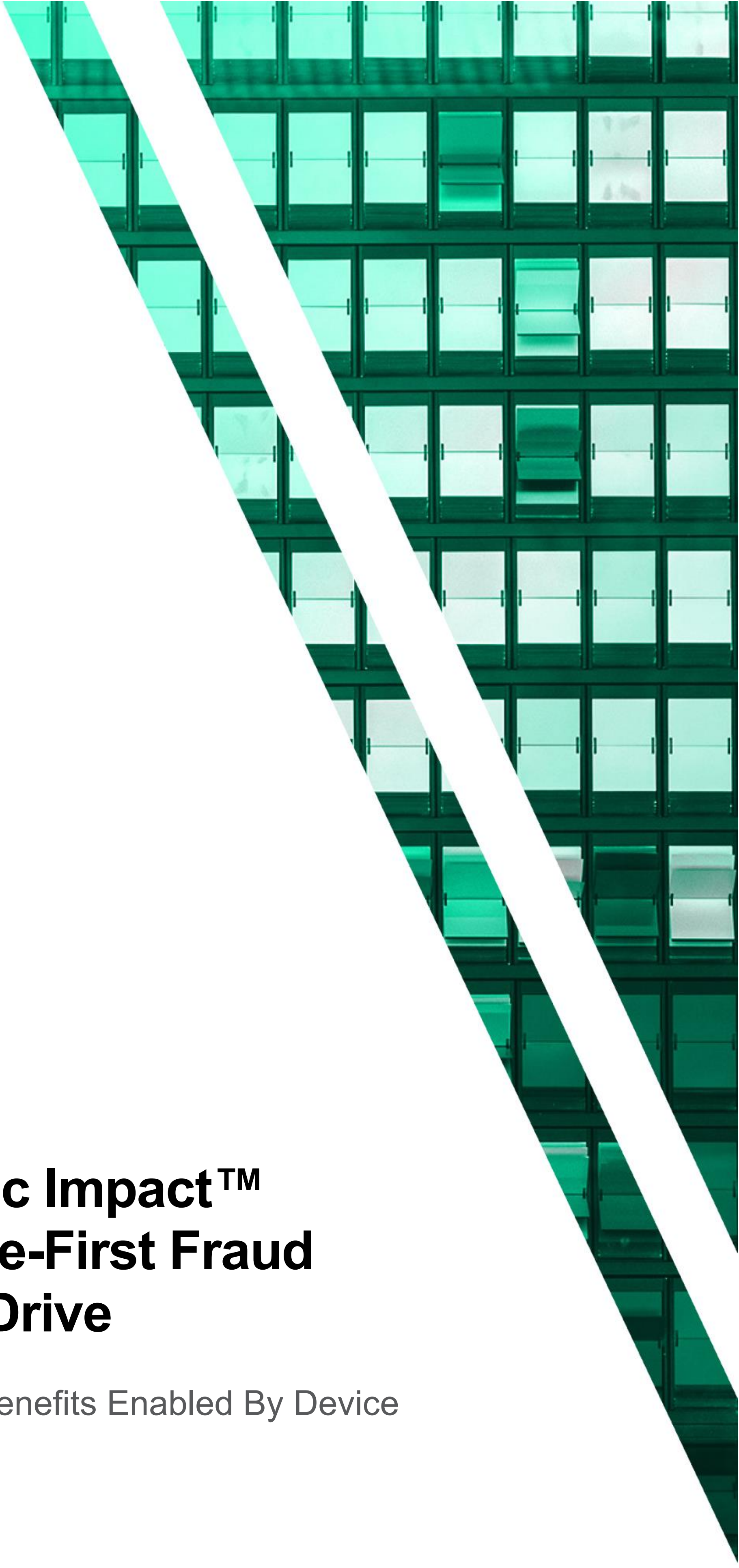
FORRESTER®



The Total Economic Impact™ Of SHIELD's Device-First Fraud Intelligence For inDrive

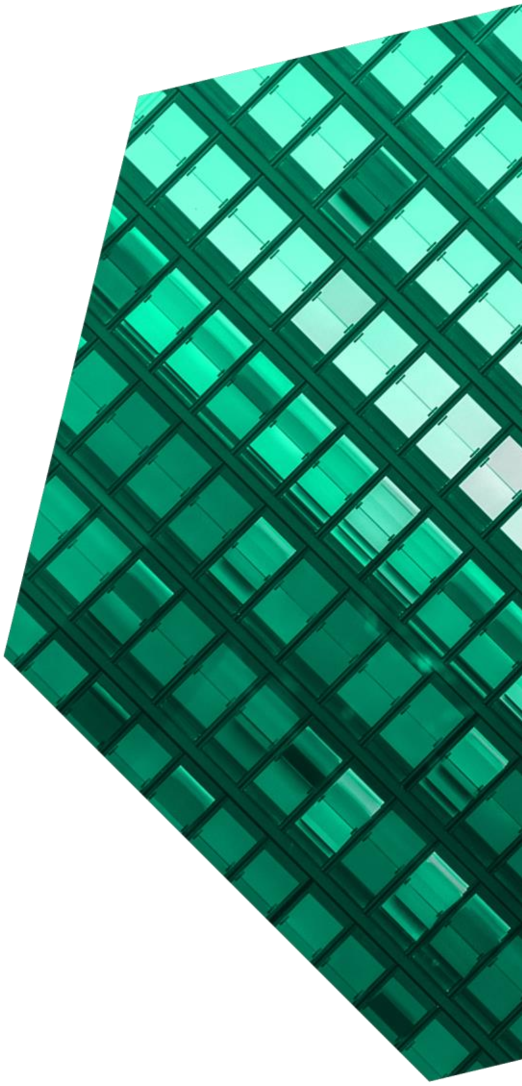
Cost Savings And Business Benefits Enabled By Device Intelligence

AUGUST 2024

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY SHIELD

Table Of Contents

Consulting Team: *Amelia Lau*
Jamie Macaulay
Line Larrivaud



Executive Summary

The democratization of AI and open-source tools has caused digital businesses to become more vulnerable to sophisticated fraud attacks, which enable fraudsters to easily conduct malicious activities at scale prior to the traditional payment and identity checks. SHIELD's device-first approach acts as the first line of defense for digital businesses without the need for any personally identifiable information — empowering organizations to build fair platforms trusted by users globally.

As digital businesses rapidly expand into new verticals, housing more services under one roof exponentially increases the attack surface that fraudsters can target. Additionally, the rise of AI has made it tougher to identify fraud, as it enables the use of deepfakes and voice-masking techniques to bypass Know Your Customer (KYC) protocols and worsen account takeover vulnerabilities, posing significant risks to both businesses and their users.

Traditional antifraud solutions tackle fraud at limited points of the user journey, focusing primarily on payments or identity verification detection, which require personally identifiable information (PII) like credit card numbers, emails, and phone numbers. However, fraudsters often exhibit malicious behavior even before making a fraudulent transaction or creating fake accounts.

SHIELD commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Device Intelligence.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Device Intelligence on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed three representatives from inDrive who have experience using Device Intelligence. Forrester used this experience to project a three-year financial analysis.

INDRIVE KEY STATISTICS

Benefits (PV)

$104.6M

Net present value (NPV)

$97.5M

Prior to using Device Intelligence, the interviewees noted they had trialed a tool that was built internally to combat fraud. However, this attempt yielded limited success and left them with blind spots as to the types of fraud being committed and an inability to eradicate problematic accounts as malicious users could easily change common identifiers such as usernames or phone numbers. These limitations led to tangible financial losses and undermined their mission statement of challenging injustice to make the world a fairer place.

After their investment in Device Intelligence, inDrive was able to enter high-risk geographical markets rapidly with greater confidence, while requiring a leaner team than was forecasted.

inDrive takes a strategic approach to tackling fraud by focusing on efficiency which allowed them to redirect resources toward sustaining growth and profitability.

SHIELD offers a device-first approach that addresses fraud at its root. As mobile operating systems pivot toward being more privacy-focused, relying on PII has become increasingly challenging for user identification. SHIELD's Device-First Fraud Intelligence provides comprehensive protection throughout the entire user journey without the need for PII, and is utilized across a wide variety of industries, including mobility, digital banking, e-wallets, e-commerce, delivery services, and gaming.

The platform comprises persistent device identification through the SHIELD Device ID, that identifies every physical device on a platform and eliminates the root of fraudulent fake accounts.

SHIELD is also capable of detecting when a good user turns bad by providing real-time actionable fraud signals intelligence on the use of malicious tools such as app cloners, emulators, GPS spoofers and more.

Key results from the investment include cost savings from reduced FTE requirement for the fraud prevention team, improved fraud officer productivity, avoided annual losses from collusion, recaptured revenue from prevention of GPS spoofing and more.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits include:

- **Reduced FTE requirement for the fraud prevention team, resulting in cost savings of $45.4 million.** SHIELD's Device Intelligence solution and clustering technology enables inDrive's fraud prevention team to initiate proactive intervention. Early identification and elimination of fraud syndicate clusters — especially in high-risk markets with unique risk profiles — offer inDrive confidence to expand into new markets aggressively while ensuring that they stay ahead of emerging threats and reduce the occurrence of fraud. This results in a decrease of 92% to 94% in operational need for FTEs that would have potentially been recruited across markets for the fraud prevention team. These FTE roles range from fraud officers, verification officers, to risk analysts, and would have been required to keep up with the escalating operational demands that come with new market entry. Over three years and a total of 63 geographical markets that inDrive has been projected to operate in, this cost avoidance amounts to a PV of $45.4 million.
- **Improved fraud officer productivity, resulting in cost savings of $290,000.** SHIELD's Device ID and fraud intelligence streamlines fraud investigation operations through real-time reporting of suspicious activities happening across devices and IP addresses, as well as the use of malicious tools. This reduces the time needed for manual investigation by allowing current teams to identify and investigate risky devices more easily. As a result, the workloads for these teams related to fraud case management and reporting were reduced by 30% to 55%. Fraud officers who previously spent up to 70% of their time on this work can now divert their attention to more value-added tasks. Overall, inDrive saves $290,000 from these operational improvements over three years.
- **Avoided $39.9 million in losses from driver-passenger collusion.** SHIELD identifies instances of fraud syndicates conducting driver-passenger collusion, where multiple driver and passenger accounts originate from the same device. These fake accounts are gateways to fraud and can be abused in a myriad of ways especially when used by fraud syndicates at scale. Early detection with Device Intelligence allows inDrive to identify and prevent cases of fake rides being completed and the potential abuse of incentives. Leveraging Device Intelligence reduces the incidence of such fraudulent accounts at inDrive by 75%, thus

avoiding $39.9 million in losses from driver and passenger collusion over three years.

- **Avoided $2 million in losses from fraudulent drivers monopolizing rides.** Another prominent fraud use case involves driver syndicates monopolizing rides by using autoclickers, app cloners, and emulators to accept ride requests quickly before other genuine drivers can submit alternative bids or accept these requests. This capability to detect and block malicious tools ensures that ride opportunities are fairly distributed among genuine drivers, preventing inDrive from experiencing losses tied to risky devices, which total $2 million over three years.

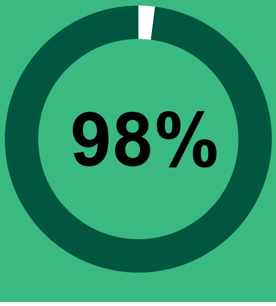
- **Recaptured $16 million in revenue from prevention of GPS spoofing.** Device Intelligence's capabilities enable inDrive to reduce the ability of fraud syndicates to manipulate the matching engine. Drivers conducting fraud can utilize GPS spoofers on multiple fake passenger accounts to drive the demand for rides in an area, making genuine passengers wait for a longer time or even potentially having to bid higher to secure a ride. SHIELD's Device Intelligence allows inDrive to pinpoint the exact moment malicious tools like GPS spoofers are activated to ensure genuine passengers get rides on time and at a fair price.

  Across a period of three years, Device Intelligence's detection of malicious tools allows inDrive to reduce the percentage of ride requests affected by GPS spoofing by 97.5%, preventing price manipulation and enabling them to recapture $16 million in revenue.

inDrive's return on its investment in SHIELD's Device-First Fraud Intelligence Platform:

13.8x

Percentage reduction of ride requests affected by GPS spoofing



- **Cost avoidance of $2.7 million from reduced need of one-time password (OTP) verification.** SHIELD's Device Intelligence solution allows inDrive to retire a legacy solution due to its enhanced ability to identify from a device level, whether a particular device or user is risky as opposed to relying solely on OTP during account creation. inDrive avoids costs worth $2.7 million over three years.

Unquantified benefits. Benefits that are not quantified in this study include:

- **Greater confidence and success in expanding into high-risk markets for growth.** Device Intelligence enables inDrive to expand into new, high-risk markets with confidence by helping them to service genuine users while preemptively preventing the occurrence of fraud.

- **Greater confidence in launching new product features.** In addition to new market entry, SHIELD's ability to combat fraudulent activity at the device level enables inDrive to adopt new product features more readily, including expansion of payment methods to improve its service.

- **Enhanced quality of inDrive's user base with more than 99.77% genuine users.** Device Intelligence was instrumental in improving inDrive's genuine user base — by not only circumventing issues that bad actors bring but also allowing for greater revenue optimization and growth opportunities through targeting genuine users.

- **Greater trust fostered in the inDrive ecosystem from elevated customer experience (CX) and driver experience.** The ability to profile devices and prevent fraud in real time builds trust with genuine customers that they can rely on inDrive for safe, transparent, and economically-fair rides, thus making for more positive CX. Drivers who were formerly beset with challenges such as ride-hogging by fraudulent accounts now benefit from a system that allocates riding opportunities equally. This allows drivers on inDrive's platform to enjoy a more equitable distribution of income, thus building trust in their platform and enhancing their employee experience (EX).

Costs. Three-year, risk-adjusted PV costs include:

- **Internal deployment and maintenance costs of $476,000.** FTE costs incurred by inDrive — not charged by SHIELD — includes an initial 600 hours of integration by three software engineers as well as one FTE to handle maintenance on an ongoing basis.

- **Solution licensing costs amounting to $6.6 million.** This is the only charge incurred by SHIELD directly. Pricing depends on many factors including volume of unique devices as well as included features and add-ons.

The interview and financial analysis found that InDrive experiences benefits of $104.6 million over three years versus costs of $7.1 million, resulting in a net present value (NPV) of $97.5 million and an ROI of 1,377%.

Forrester recommends the reader to note inDrive's status as a high-growth ride-hailing company. The magnitude of these results may therefore not be replicable in your context.

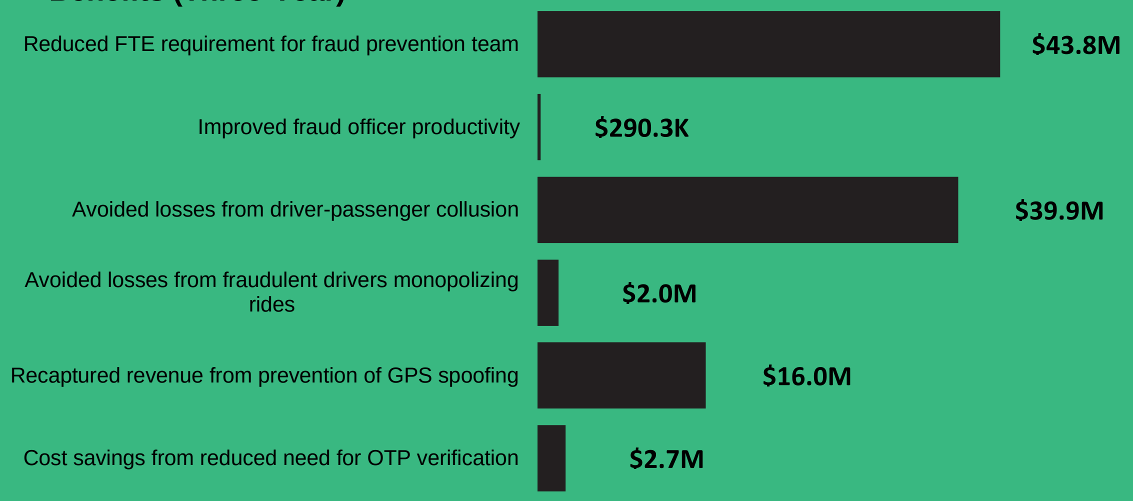
ROI
1,377%

BENEFITS PV
$104.6M

NPV
$97.5M

PAYBACK
<6 months

Benefits (Three-Year)



> **“SHIELD helps us protect our ride-hailing business against the risks presented by fraud. Turning it off for just a month would result in a surge of suspicious user activity.”**
>
> — Head of fraud prevention

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Device Intelligence.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Device Intelligence can have on an organization.

DUE DILIGENCE

Interviewed SHIELD stakeholders and Forrester analysts to gather data relative to Device Intelligence.

INTERVIEW

Interviewed three representatives from inDrive to obtain data with respect to costs, benefits, and risks.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by SHIELD and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Device Intelligence.

SHIELD reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

SHIELD provided the customer name for the interview but did not participate in the interview.

The SHIELD Device Intelligence Customer Journey

🟩 Drivers leading to the Device Intelligence investment

INTERVIEWEE'S ORGANIZATION

Forrester interviewed three representatives from inDrive who have experience with SHIELD Device Intelligence. Their organization has the following characteristics:

- Offers ride-hailing services.
- Present in 655 cities across 46 countries.
- Fares negotiated directly between driver and rider via a bidding system.
- Global team of 31 FTEs in the fraud prevention team.

KEY CHALLENGES

inDrive's first venture into fraud prevention involved piloting an internally built minimum viable product (MVP) using open-source library material. The senior product manager of inDrive shared, "We summarized all our potential costs and potential risks [from building an internal tool] and came to the conclusion that we may invest all these resources and end up with a solution that's not really good."

The interviewees noted that even with an internal MVP, inDrive continued to struggle with common challenges, including:

- **Poor visibility and understanding on the types of fraud use cases and scale of fraud.** In-house solutions still relied on rule-based programming which was insufficient to identify and manage emerging types of fraud prior to an attack. inDrive's senior product manager explained: "While we have always understood that we have different kinds of fraud in ride-hailing, we were not able to correctly evaluate them before integration. Rather, they existed only as various hypotheses."
- **Difficulty eradicating fraudulent accounts and activities.** Traditional methods of authentication such as user IDs, phone numbers, and email addresses can be easily obtained and interchanged rapidly. This made it difficult to block fraudulent entities and activities permanently. It also presented challenges in eradicating fraud syndicates that could just create new fraudulent accounts flexibly at scale to replace blocked accounts. The senior product manager of inDrive said: "[Before device fingerprinting] we mainly relied on user ID, phone, etc. But all these IDs are unstable, and users can easily change them."
- **Lack of tools to scale fraud prevention efforts to meet the demands from their expansion into new markets.** inDrive's aggressive expansion into 10 new markets every year on average understandably causes the company to face a mushrooming of accounts, including fraudulent ones. The scale of inDrive's growth resulted in internal teams lacking adequate tools to help them proactively deal with malicious activities and fake accounts. The director of ride-hailing for APAC stated: "With much of our business operating in environments where fraud can pose a serious concern, fraud protection and prevention are critically important. inDrive has been growing rapidly in the last 10 years. During this time, we have had to increase the capacity of our fraud prevention team and intelligence team fast, which has been very tough."
- **Living up to the company's mission to challenge injustice to build trust within the ecosystem.** inDrive uniquely positions itself in the industry as a people-driven business on a mission to challenge injustice. inDrive's negotiation and bidding system aims to ensure that prices are kept transparent, and drivers are

fairly compensated. Yet, the company faced difficulties in upholding this promise and maintaining trust with their users due to the proliferation of fraudulent accounts and activities. inDrive's senior product manager said: "One of inDrive's key values is to give our users equal opportunities. With [fraudsters tapping on tools like] third-party applications, this equilibrium is disrupted with fraudsters potentially earning two to four times more than genuine drivers."

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

inDrive searched for a solution that could:

- Address technical requirements.
- Offer competitive pricing.
- Scale rapidly to process a growing volume of accounts and transactions as it expanded geographically.
- Establish credibility with its experience of working with large corporates.

After a request for proposal (RFP) and business case process evaluating multiple vendors, inDrive chose SHIELD's Device Intelligence solution and began deployment:

- Device Intelligence was integrated globally from the start, since incorporating the software development kit (SDK) in only a few markets could still lead to circumvention using virtual private networks (VPNs).
- Device Intelligence was deployed with no switch-off tool. The only way to disable the SDK is to remove it completely.

> **"SHIELD met all our requirements — ability to work under high loads, be a stable long-term partner for us, and offer competitive pricing."**
>
> *Senior product manager*

USE CASE DESCRIPTION

For this case study, Forrester has modeled benefits and costs over three years.

Some key points for Forrester's modeling of inDrive are as follows:

Key Metrics

- **Hyperscaler with a high new market entry rate**
- **Average cost of a fraudulent account was $2.50**
- **Over $40 million in savings from reduced FTE requirement over three years**

Total Benefits

Ref.	Benefit	Year 1	Year 2	Year 3	Total	Present Value
Atr	Reduced FTE requirement for fraud prevention team	$13,317,615	$17,212,500	$23,276,970	$53,807,085	$43,820,461
Btr	Improved fraud officer productivity	$79,552	$123,019	$154,867	$357,438	$290,342
Ctr	Avoided losses from driver-passenger collusion	$10,500,000	$15,600,000	$23,190,000	$49,290,000	$39,861,007
Dtr	Avoided losses from fraudulent drivers monopolizing rides	$525,000	$780,000	$1,159,500	$2,464,500	$1,993,050
Etr	Recaptured revenue from prevention of GPS spoofing	$6,113,250	$6,435,000	$6,756,750	$19,305,000	$15,952,128
Ftr	Cost savings from reduced need for OTP verification	$192,000	$1,140,000	$2,070,000	$3,402,000	$2,671,916
	Total benefits (risk-adjusted)	$30,727,417	$41,290,519	$56,608,087	$128,626,023	$104,588,904

REDUCED FTE REQUIREMENT FOR FRAUD PREVENTION TEAM

Evidence and data. Device Intelligence could accurately identify the devices behind fake account creation and also pinpoint potential fraud syndicates. Interviewees from inDrive noted that having a dashboard of such information and data was critical in arming them with the insights to initiate proactive intervention. This ability to zero in on emerging threat clusters was key to inDrive’s confidence and success in expanding into new markets, especially those perceived to be of greater risk with diverse fraudulent use cases.

- The director of ride-hailing for APAC noted: “Fraud is happening everywhere in the world, but more so in Asia Pacific, the fraud community is very fast-moving, dynamic, and creative. Once we had gotten to a certain level of expansion and acquired a huge base of users, it started to be very hard to prevent fraud just by ourselves and that's how we came to the SHIELD partnership.”
- Leveraging Device Intelligence has allowed inDrive to expand into 46 markets by Year 2 of deployment while maintaining a lean 31- to 40-member FTE prevention team across the years. Without the solution, the company would have needed to hire more than 600 FTEs to handle the load of preventing fraud across the 60 markets they are projected to operate in by the end of Year 3.
- inDrive’s senior product manager shared: “Our antifraud team is lean and diligent. Without SHIELD, we would have needed much more people and time to combat fraud.”

Modeling and assumptions. In modeling the benefit, Forrester has deemed the following:

- inDrive expands into an average of 10 to 15 new markets per year.
- An average of 10 FTEs would have been required to work in the fraud prevention team, including fraud officers, verification, and risk analysts, etc. per market without the use of Device Intelligence.

Risks. The potential benefit to be realized for prospective customers may differ according to the following:

- The scale of fraud across industries and regions.
- The size of fraud prevention team required may vary across industries and companies of different sizes.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $43.8 million.

> **“One of our competitors has 200 fraud specialists just for one market. Taking that to gauge the team size that would have been needed without SHIELD, it’s huge. These specialists are also costly and hard to recruit.”**
>
> *Head of fraud prevention*

Reduced FTE Requirement For Fraud Prevention Team

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Geographical markets	Y1: Interview; Y2 and Y3: PYx1.3	37	46	60
A2	Average number of FTEs required to work in the fraud prevention team per market without Device Intelligence	TEI standard	10	10	10
A3	Total FTEs required to work in the fraud prevention team without Device Intelligence	A1*A2	370	460	598
A4	Average unburdened FTE annual salary	Y2: TEI standard Y1: Y2*0.97 Y3: Y2*1.03	$48,500	$50,000	$51,500
A5	Fully-burdened labor rate	TEI standard	135%	135%	135%
A6	Average fully-burdened FTE annual salary	A4*A5	$65,475	$67,500	$69,525
A7	**Subtotal: Potential FTE cost of fraud prevention prior to Device Intelligence**	**A3*A6**	**$24,225,750**	**$31,050,000**	**$41,575,950**
A8	Total FTEs required to work in the fraud prevention team with Device Intelligence	Interviews	31	35	40
A9	**Subtotal: FTE cost of fraud prevention with Device Intelligence**	**A6*A8**	**$2,029,725**	**$2,362,500**	**$2,781,000**
A10	Reduction in FTE requirement with Device Intelligence	A7-A9	$22,196,025	$28,687,500	$38,794,950
A11	Attribution ratio	TEI standard	75%	75%	75%
At	Reduced FTE requirement for fraud prevention team	A10*A11	$16,647,019	$21,515,625	$29,096,213
	Risk adjustment	↓20%			
Atr	Reduced FTE requirement for fraud prevention team (risk-adjusted)		$13,317,615	$17,212,500	$23,276,970

Three-year total: $53,807,085 **Three-year present value: $43,820,461**

IMPROVED FRAUD OFFICER PRODUCTIVITY FROM DEVICE ID

Evidence and data. Device Intelligence identifies trustworthy devices, users, and accounts through SHIELD’s Device ID which identifies the root of fraud and SHIELD’s fraud intelligence which identifies the exact moment of activation of malicious tools happening across devices in real time. The interviewees stated that this streamlined their fraud investigation operations as it reduced workloads for the nine fraud officers whose responsibilities primarily revolved around fraud case management and reporting.

- Interviewees said that by Year 3, the share of hours allocated to fraud case management and reporting had been reduced from 70% to 15%.
- inDrive’s director of ride-hailing for APAC shared: “After implementing SHIELD, we could create optimal automatization of identification, flags, and other manual work that is part of the daily routine of our fraud officers. This used to take up about

70% of their time previously and now, with SHIELD, it's around 30%."

Modeling and assumptions. For the purposes of the case study, Forrester assumes the following:

- Each fraud officer works 2,080 hours annually.
- Average fully-burdened hourly rate per fraud officer is $33.43 by Year 3.
- Productivity recapture rate of 50%, which enables inDrive to save at least 600 hours per fraud officer from enhanced productivity enabled by SHIELD Device ID.

Risks. The potential benefit to be realized for prospective customers may differ according to the following:

- The scale of fraud across industries.
- Complexity of fraud cases.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $290,000.

> **"The productivity of each product officer has increased after implementing SHIELD as it has helped to reduce the time spent on simple procedures by at least half. Now, they can focus on more value-added activities."**
>
> *Head of fraud prevention*

Improved Fraud Officer Productivity

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	FTE fraud officers	Interviews	9	9	9
B2	Annual hours worked per FTE	TEI standard	2,080	2,080	2,080
B3	Average fully-burdened FTE hourly rate	A6/B2	$31.48	$32.45	$33.43
B4	Share of hours allocated to fraud case management and reporting (pre-implementation)	Interviews	70%	70%	70%
B5	Share of hours allocated to fraud case management and reporting (post-implementation)	Interviews	40%	25%	15%
B6	**Subtotal: Net decrease in time spent on fraud case management and reporting**	**B4-B5**	**30%**	**45%**	**55%**
B7	Hours reassigned per FTE	B2*B6	624	936	1,144
B8	Productivity recapture rate	TEI standard	50%	50%	50%
B9	Attribution ratio	TEI standard	100%	100%	100%
Bt	Improved fraud officer productivity	B1*B3*B7*B8*B9	$88,391	$136,688	$172,074
	Risk adjustment	↓10%			
Btr	Improved fraud officer productivity (risk-adjusted)		$79,552	$123,019	$154,867
	Three-year total: $357,438		**Three-year present value: $290,342**		

AVOIDED LOSSES FROM DRIVER-PASSENGER COLLUSION

Evidence and data. Fraud syndicates often use malicious tools like app cloners, emulators, and autoclickers to create multiple fake driver and passenger accounts from the same devices to conduct attacks at scale. SHIELD Device ID enabled employees at inDrive to identify instances of multiple driver and passenger accounts originating from the same SHIELD Device ID and pinpoint driver-passenger collusion.

- The interviewees stated that there was a post-implementation reduction in fraudulent accounts used for collusion from 4% to 1% of the user base and that the cost to inDrive per fraudulent account is approximately $2.50.

Modeling and assumptions. For this benefit, all data points came directly from interviews.

- Annual reduction in the number of fraudulent accounts involved in driver-passenger collusion scales year-over-year from 10.5 million in Year 1 to 23.3 million by Year 3.

Risks. Organizations may realize results different to those presented in the financial model due to:

- Difference in percentage of fraudulent accounts before implementation.
- Difference in size of total user base.
- Difference in average cost to the organization per fraudulent account.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $39.9 million.

Avoided Losses From Driver-Passenger Collusion

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average percentage of fraudulent accounts used for driver-passenger collusion among user base (pre-implementation)	Interviews	4%	4%	4%
C2	Average percentage of fraudulent accounts used for driver-passenger collusion among user base (post-implementation)	Interviews	1%	1%	1%
C3	Reduction in percentage of fraudulent accounts among user base involved in driver-passenger collusion after implementing Device Intelligence	C1-C2	3%	3%	3%
C4	**Subtotal: Annual reduction in number of fraudulent accounts among user base involved in driver-passenger collusion**	**Interviews**	**10,500,000**	**15,600,000**	**23,190,000**
C5	Average cost of a fraudulent account to inDrive	Interviews	$2.50	$2.50	$2.50
C6	Attribution ratio	TEI standard	50%	50%	50%
Ct	Avoided losses from driver-passenger collusion	C4*C5*C6	$13,125,000	$19,500,000	$28,987,500
	Risk adjustment	↓20%			
Ctr	Avoided annual losses from driver-passenger collusion (risk-adjusted)		$10,500,000	$15,600,000	$23,190,000
	Three-year total: $49,290,000			**Three-year present value: $39,861,007**	

AVOIDED LOSSES FROM FRAUDULENT DRIVERS MONOPOLIZING RIDES

Evidence and data. Fraudulent drivers can use autoclicking tools to shut genuine drivers out of the lucrative intercity market by accepting rides instantaneously. SHIELD's Device Intelligence flags the exact tools being used to mitigate this impact.

- The interviewees stated that there was a post-implementation reduction in fraudulent accounts used for monopolization from 4% to 1% of the user base, and that the cost to inDrive per fraudulent account is approximately $2.50.

Modeling and assumptions. For this benefit, all data points came directly from interviews.

- Annual reduction in the number of fraudulent accounts involved in intercity monopolization starts at just over 50,000 in Year 1, scaling with total user base growth in subsequent years.

Risks. Organizations may realize results different to those presented in the financial model due to:

- Difference in average percentage of users who carry out intercity rides.
- Difference in size of total user base.
- Difference in average cost to the organization per fraudulent account.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $2 million.

Avoided Losses From Fraudulent Drivers Monopolizing Rides

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Users carrying out intercity rides across markets	Interviews	1,750,000	2,600,000	3,865,000
D2	Average percentage of fraudulent accounts monopolizing intercity rides among user base (pre-implementation)	Interviews	4%	4%	4%
D3	Average percentage of fraudulent accounts monopolizing intercity rides among user base (post-implementation)	Interviews	1%	1%	1%
D4	Reduction in percentage of fraudulent accounts among user base involved in monopolizing intercity rides after implementing Device Intelligence	D2-D3	3%	3%	3%
D5	**Subtotal: Annual reduction in number of fraudulent accounts among user base involved in monopolizing intercity rides**	**D1*D4*10**	**525,000**	**780,000**	**1,159,500**
D6	Average cost of a fraudulent account used to monopolize rides	Interviews	$2.50	$2.50	$2.50
D7	Attribution ratio	TEI standard	50%	50%	50%
Dt	Avoided losses from fraudulent drivers monopolizing rides	D5*D6*D7	$656,250	$975,000	$1,449,375
	Risk adjustment	↓ 20%			
Dtr	Avoided losses from fraudulent drivers monopolizing rides (risk-adjusted)		$525,000	$780,000	$1,159,500
	Three-year total: $,2464,500			**Three-year present value: $1,993,050**	

RECAPTURED REVENUE FROM PREVENTION OF GPS SPOOFING

Evidence and data. Fraud syndicates utilize fake accounts and GPS spoofing to generate artificial demand in a location to increase bids for a ride and be deceptive as to their drivers' real location.

- The interviewees mentioned that GPS-spoofing drivers' locations in particular led to significant losses due to cancelled rides.
- The interviewees mentioned that implementing Device Intelligence reduced instances of GPS spoofing significantly, from 4% of rides to 0.10%.

Modeling and assumptions. For this study, Forrester assumes:

- Twenty-five percent of rides affected by GPS spoofing are cancelled due to excessive wait times.
- The average cost per ride across markets is $5.
- The average commission rate due to be received by inDrive is 10%.

Risks. Organizations may realize results different to those presented in the financial model due to:

- Difference in total number of driver accounts across markets.
- Difference in average number of ride requests.
- Difference in instances of GPS spoofing before implementing Device Intelligence.
- Difference in percentage of ride cancellation.
- Difference in average cost per ride across markets.
- Difference in average commission rate.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $16 million.

> **"Cost savings from stopping fraud loss can be used instead to expand into new verticals safely, unlocking more revenue opportunities with risk of an increased surface area for fraud attacks. As a result, our path to profitability is twice as fast."**
>
> *Head of fraud prevention*

Recaptured Revenue From Prevention Of GPS Spoofing

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Driver accounts across all markets	Y2: Interviews Y1: Y2*0.95 Y3: Y2*1.05	4,750,000	5,000,000	5,250,000
E2	Average number of ride requests per month for each driver account	Interviews	55	55	55
E3	Average percentage of ride requests affected by GPS spoofing (pre-implementation)	Interviews	4%	4%	4%
E4	Average percentage of ride requests affected by GPS spoofing (post-implementation)	Interviews	0.1%	0.1%	0.1%
E5	Reduction in percentage of fraudulent accounts among user base involved in GPS spoofing after implementing Device Intelligence	E3-E4	3.9%	3.9%	3.9%
E6	Average percentage of ride requests affected by GPS spoofing that get cancelled due to long waiting time	Interviews	25%	25%	25%
E7	**Subtotal: Average number of ride requests annually affected by GPS spoofing that get cancelled due to long waiting time**	**E1*E2*E5*E6*12**	**30,566,250**	**32,175,000**	**33,783,750**
E8	Average cost per ride	Interviews	$5	$5	$5
E9	Average commission rate for drivers	Interviews	10%	10%	10%
E10	Attribution ratio	TEI standard	50%	50%	50%
Et	Recaptured revenue from prevention of GPS spoofing	E7*E8*E9*E10	$7,641,563	$8,043,750	$8,445,938
	Risk adjustment	↓ 20%			
Etr	Recaptured revenue from prevention of GPS spoofing (risk-adjusted)		$6,113,250	$6,435,000	$6,756,750
	Three-year total: $19,305,000			**Three-year present value: $15,952,128**	

COST SAVINGS FROM REDUCED NEED FOR OTP VERIFICATION

Evidence and data. Prior to Device Intelligence, one-time passwords (OTP) were used to verify accounts upon creation. Implementing SHIELD Device Intelligence reduced the need for this method.

- inDrive previously utilized a third-party vendor to support OTP, which became redundant upon deploying SHIELD Device Intelligence.
- The senior product manager stated: “SHIELD has helped us reduce costs spent on other services. For example, in some countries, we use another vendor to target SMS fraud by paying for every check. When we deployed SHIELD in these countries, we were able to switch off [the services of] this vendor and still withstand different kinds of fraud.”
- The interviewees estimated that the budget for OTP was around 3% of inDrive’s annual revenue.

Modeling and assumptions. For this study, Forrester assumes:

- Budget allocation required for pre-implementation OTP increases by around 20% year over year.

Risks. Organizations may realize results different to those presented in the financial model due to:

- Difference in budget allocation to OTP and/or other verification tools.
- Difference in post-implementation requirements.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $2.7 million.

Cost Savings From Reduced Need For OTP Verification

Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	Budget for OTP verification during registration and login	Interviews	$2,400,000	$2,850,000	$3,450,000
F2	Percentage of OTP verification expense needed pre-implementation	Interviews	100%	100%	100%
F3	Percentage of OTP verification expense needed post-implementation	Interviews	90%	50%	25%
F4	Percentage reduction in OTP verification expense needed	F2-F3	10%	50%	75%
F5	Attribution ratio	TEI standard	100%	100%	100%
Ft	Cost savings from reduced need for OTP verification	F1*F4*F5	$240,000	$1,425,000	$2,587,500
	Risk adjustment	↓20%			
Ftr	Cost savings from reduced need for OTP verification (risk-adjusted)		$192,000	$1,140,000	$2,070,000
	Three-year total: $3,402,000		**Three-year present value: $2,671,916**		

UNQUANTIFIED BENEFITS

Interviewees from inDrive mentioned the following additional benefits that their organization experienced but was not able to quantify:

- **Greater confidence and success in expanding into high-risk markets for growth.** The interviewees said that Device Intelligence enabled their organization to expand into new, high-risk markets with confidence by helping them to focus their resources on genuine users while preemptively preventing the occurrence of fraud. Interviewees noted that expansion into new markets used to be a key challenge and experienced failures in select markets before adopting Device Intelligence.

  The director of ride-hailing for APAC stated: “The top three things coming out of our partnership with SHIELD from a business perspective are service quality, cost reduction, and confidence to scale. Once we reduce fraud, we get higher customer satisfaction, retention, and hence, revenues.”

- **Greater confidence in launching new product features.** Beyond new market entry, SHIELD’s ability to combat fraudulent activity at the device level has allowed inDrive to adopt new product features more readily, including expanding payment methods and improving their customer service.

- **Enhanced quality of inDrive's user base with more than 99.77% genuine users.** Interviewees said that Device Intelligence was instrumental in improving the genuine user base of their organization as it circumvented issues that bad actors bring and also allowed for greater revenue optimization and growth opportunities by targeting genuine users. The senior product manager noted: "SHIELD gives us the opportunity to evaluate the number of users of third-party apps within inDrive. While this was a challenge before the SHIELD integration, this was not something we could assess. Now with SHIELD, we can understand with 99.9% accuracy the users on third-party applications as compared to the original inDrive application."

  The director of ride-hailing for APAC also stated: "Before SHIELD, in certain countries, the amount of fraud amounted to 50% of our overall volumes in the country. Very quickly, with the SHIELD implementation, we reduced the amount of fraud to less than 1%."

- **Greater trust fostered in the inDrive ecosystem from elevated CX and driver experience.** The ability to profile devices and prevent fraud in real time built trust with genuine customers that they can rely on inDrive for safe, transparent, and economically-fair rides, thus making for more positive CX. Drivers who were formerly beset with challenges such as ride-hogging by fraudulent accounts now benefit from a system that allocated ride opportunities equally. This allowed inDrive's drivers to enjoy a more equitable distribution of income, thus building trust in their platform and enhancing EX.

  inDrive's director of ride-hailing for APAC explained: "From a customer lifetime value perspective, implementing SHIELD has helped to improve user experience, user satisfaction, and the quality of the user flow. This is reflected in how user retention is growing, and they come to us more often. As a result, we don't have to acquire new ones, we just have to retarget current users, and with that, we see that the lifetime value for the user grows exponentially."

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Device Intelligence and later realize additional uses and business opportunities, including:

- **Ability to scale more securely.** Interviewees from inDrive highlighted that the use of Device Intelligence enabled them to scale in existing markets faster than would have been possible without the solution.

- **Greater investor confidence.** Interviewees credited SHIELD with improving their security posture, which was crucial in cementing their reputation as a safe solution that investors may choose to invest in.

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

> **"We are growing fast, and it tells potential investors that we have a trusted partner to maintain a safe solution. This builds on the global reputation of our company."**
>
> *Director of ride-hailing, APAC*

Analysis Of Costs

🟩 Quantified cost data

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Gtr	Internal deployment and maintenance costs	$47,023	$167,903	$172,940	$178,128	$565,994	$476,418
Htr	Solution licensing costs	$0	$2,443,390	$2,663,295	$2,902,991	$8,009,675	$6,603,393
	Total costs (risk-adjusted)	$47,023	$2,611,292	$2,836,235	$3,081,119	$8,575,669	$7,079,811

INTERNAL DEPLOYMENT AND MAINTENANCE COSTS

Evidence and data. SHIELD does not charge a separate fee for integration and maintenance. However, inDrive incurred internal costs for integration with their existing ecosystem and ongoing maintenance.

- Three software engineer FTEs were utilized for a combined total of 600 hours for initial deployment.
- One software engineer FTE is required for ongoing maintenance.

Modeling and assumptions. For this study, Forrester assumes:

- The average annual salary of a software engineer is $75,000.
- Seniority level adjustment of 40%.

Risks. Organizations may realize results different to those presented in the financial model due to:

- Difference in internal preparation requirements.
- Difference in local software engineer salary.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $476,000.

Internal Deployment And Maintenance Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	FTEs required for deployment	Interviews	3			
G2	Hours spent on integration per FTE for deployment	Interviews	200			
G3	**Subtotal: Hours required to deploy SHIELD Device Intelligence**	**G1*G2**	**600**			
G4	Average annual unburdened FTE salary	TEI standard	$75,000			
G5	Fully-burdened labor rate	TEI standard	135%			
G6	Average annual fully-burdened FTE salary	G4*G5	$101,250			
G7	Annual hours per year	TEI standard	2,080			
G8	Average fully-burdened FTE hourly rate	G6/G7	$48.68			
G9	Senior level adjustment	TEI standard	40%			
G10	Adjusted fully-burdened hourly rate	G8*(1+G9)	$68.15			
G11	**Subtotal: Internal initial costs for solution deployment**	**G3*G10**	**$40,889**			
G12	FTE software engineers required for maintenance	Interviews		1	1	1
G13	Average number of hours dedicated to maintaining Device Intelligence per FTE annually	TEI standard		2,080	2,080	2,080
G14	Adjusted fully-burdened FTE hourly rate	Y1: G10*1.03, Y2 to Y3: PY*1.03		$70.19	$72.30	$74.47
G15	**Subtotal: Annual cost of internal support and maintenance of solution**	**G12*G13*G14**		**$146,003**	**$150,383**	**$154,894**
Gt	Internal deployment and maintenance costs	G11+G15	$40,889	$146,003	$150,383	$154,894
	Risk adjustment	↑15%				
Gtr	Internal deployment and maintenance costs (risk-adjusted)		$47,023	$167,903	$172,940	$178,128
	Three-year total: $565,994			**Three-year present value: $476,418**		

SOLUTION LICENSING COSTS

Evidence and data. inDrive pays an annual licensing fee that covers all of Device Intelligence's functionalities with no additional, hidden charges.

Modeling and assumptions. Licensing fees are unique to inDrive's requirements.

- Pricing may vary. Contact a SHIELD representative for additional details.

Risks. Organizations may realize results different to those presented in the financial model due to:

- Difference in number of unique devices monitored.

- Difference in features and add-ons purchased.

Results. To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV of $6.6 million.

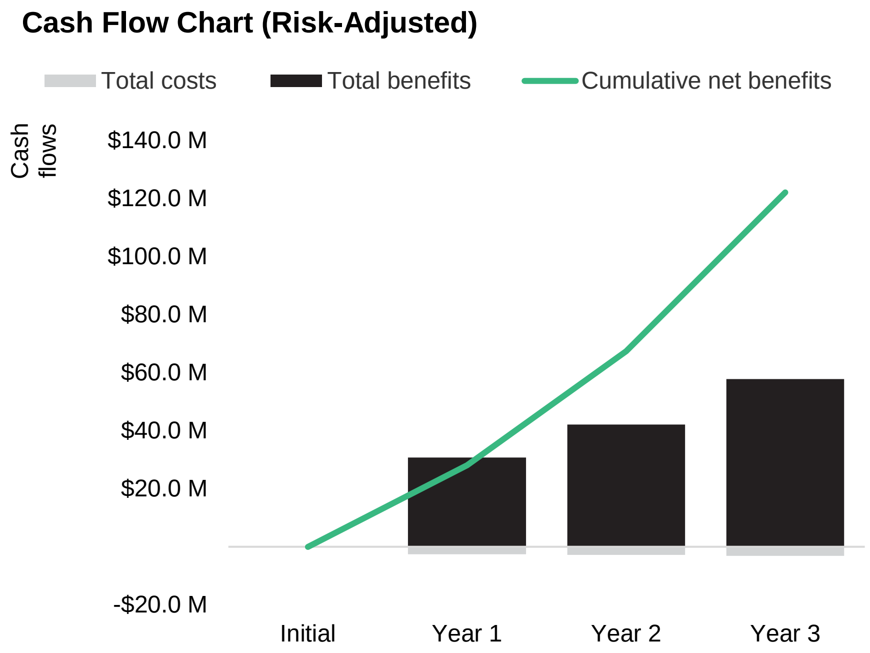
> **“One of our key decision-making factors was the pricing model as we are paying for every unique customer. This helps our growth to become more cost-efficient.”**
>
> *Head of fraud prevention*

Solution Licensing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Licensing fees	Interviews		$2,036,158	$2,219,412.22	$2,419,159.32
Ht	Solution licensing costs	Interviews		$2,036,158	$2,219,412.22	$2,419,159.32
	Risk adjustment	↑20%				
Htr	Solution licensing costs (risk-adjusted)		$0	$2,443,390	$2,663,295	$2,902,991
	Three-year total: $8,009,675			**Three-year present value: $6,603,393**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($47,023)	($2,611,292)	($2,836,235)	($3,081,119)	($8,575,669)	($7,079,811)
Total benefits	$0	$30,727,417	$41,290,519	$56,608,087	$128,626,023	$104,588,904
Net benefits	($47,023)	$28,116,125	$38,454,284	$53,526,968	$120,050,354	$97,509,093
ROI						1377%
Payback period (months)						<6

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

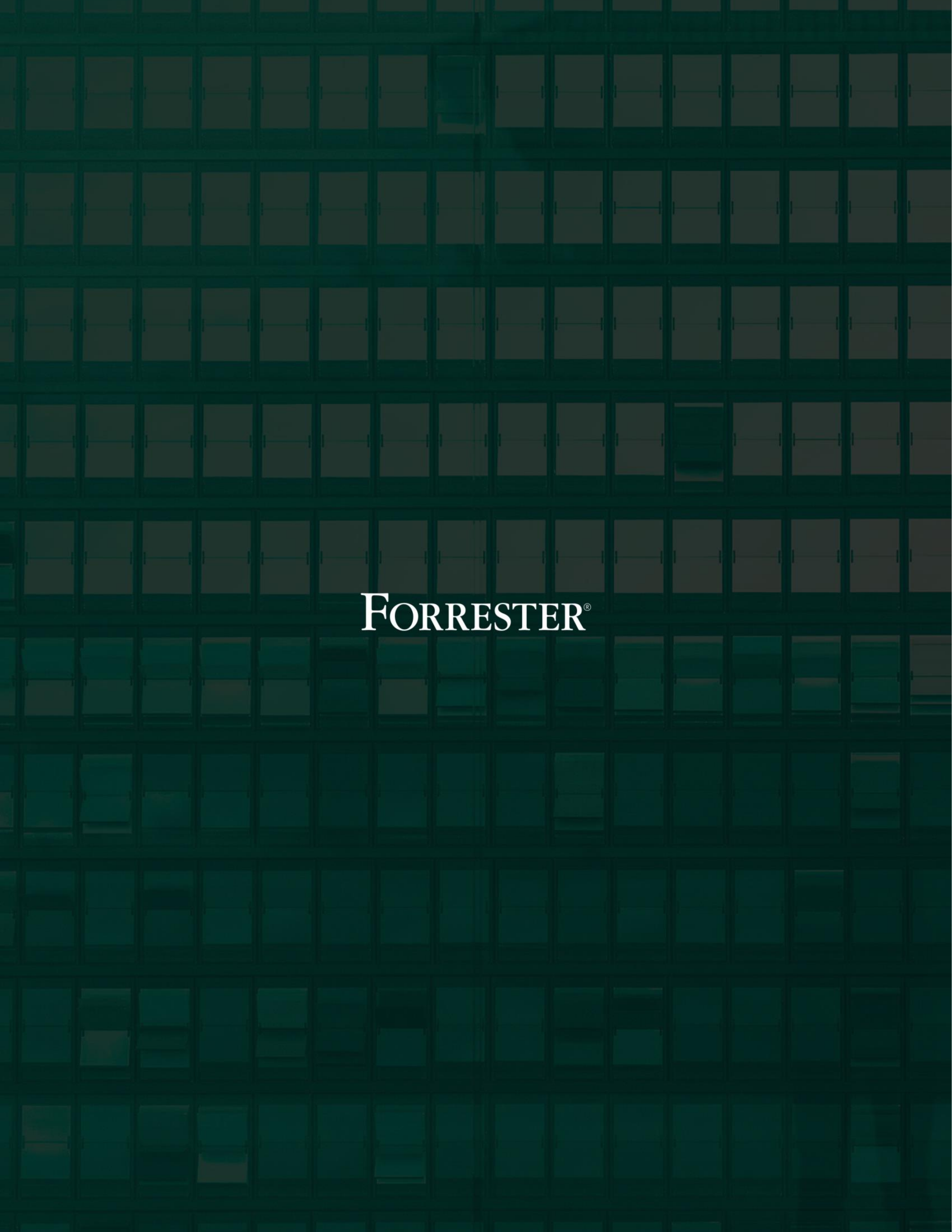
The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.



FORRESTER®