FORRESTER®

# The Total Economic Impact™ Of Group-IB Fraud Hunting Platform For A Customer Migrating From A Legacy Anti-Fraud Solution

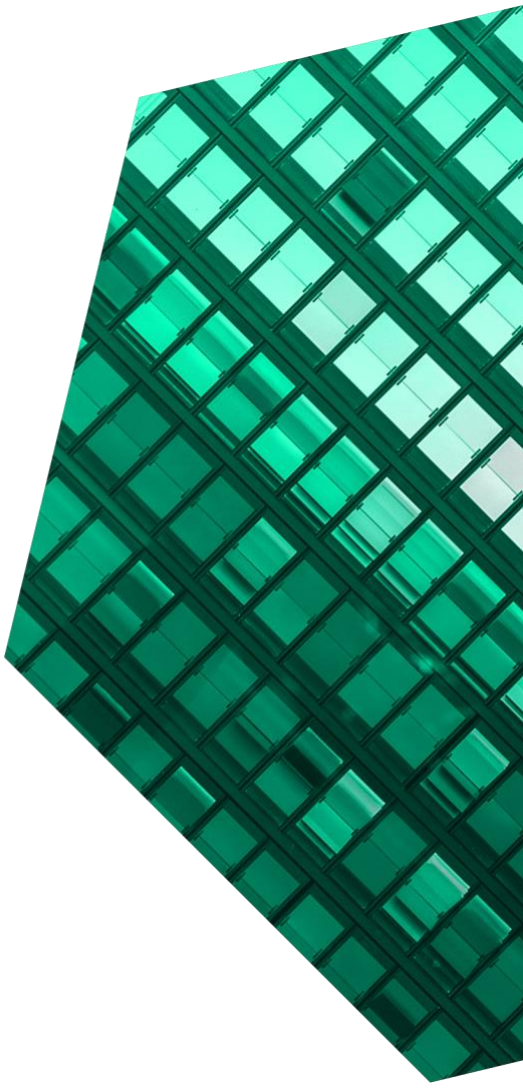
Cost Savings And Business Benefits
Enabled By Group-IB Fraud Hunting Platform

**JUNE 2021**

## Table Of Contents




*Consulting Team: Sanny Mok*

# Executive Summary

Security leaders face heightening pressure on multiple fronts as they tackle fraud. Regulators are creating stronger requirements for firms to reduce financial crime, such as fraud, while customers are constantly raising their expectations for a smooth digital experience. As businesses strive to maintain regulatory compliance while preserving customer experience and keeping operating costs in check, leaders turn to enterprise fraud management solutions to achieve this goal.

Group-IB Fraud Hunting Platform performs real-time session and user behavior data analysis on web and mobile channels to help organizations accurately detect and efficiently prevent fraud.

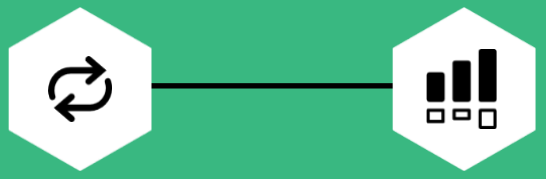
Group-IB commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Fraud Hunting Platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Fraud Hunting Platform (FHP) on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed an organization with experience using Fraud Hunting Platform. Forrester used this experience to project a three-year financial analysis.

Prior to using Fraud Hunting Platform, the customer tackled fraudulent activities using a legacy anti-fraud solution. However, the legacy system generated a high number of false positives, which masked the transactions that were truly fraudulent. The organization could not detect and prevent fraud attacks in time.

After the investment in Fraud Hunting Platform, the organization blocked more fraud attempts. The number of false positives dropped, enabling the organization to focus on the truly risky transactions and block more fraud attempts. Efficiency of fraud analysts and customer service teams improved, and costs associated to fraud reduced. Replacing the legacy solution also yielded cost savings in technology spend.

**KEY STATISTICS**



Return on investment (ROI)
**130%**

Net present value (NPV)
**$639K**

**KEY FINDINGS**

**Quantified benefits.** Risk-adjusted present value (PV) quantified benefits include:

- **Improved fraud detection represents $288K in cost savings.** The organization detected and prevented fraudulent activities more accurately and efficiently, reducing the financial impact of successful fraud attacks.
- **Improved efficiency by reducing false positives represents $336K in benefits.** The organization reduced false positives by 20% to 30%, enabling fraud analysts and call center operators to focus on transactions with higher risks.
-

- **Avoided legacy solution licensing fees represent $508K in benefits**. The organization replaced its legacy anti-fraud solution, which was 30% more costly than Fraud Hunting Platform.

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

- **Improved customer experience.** With the data FHP collected, organizations whitelisted customers, which ensured security without creating unnecessary customer friction.
- **Maintain customer trust and mitigate reputation risk.** Minimizing the number of fraud cases helped build customer trust and safeguard the reputation of organizations.

**Costs.** Risk-adjusted PV costs include:

- **Licensing cost of $441K in present value.** Annual licensing cost is $167K in Year 1 and Year 2, increasing to $175 in Year 3 to align with business growth.
- **Implementation and ongoing running cost of $51k in present value.** This includes internal effort and professional services cost incurred during implementation, and ongoing internal effort maintaining the solution.

The interview and financial analysis found that this customer experienced benefits of $1.13M over three years versus costs of $493K, adding up to a net present value (NPV) of $639K and an ROI of 130%.

**Fraud Hunting Platform helps us focus on the riskier transaction by eliminating false positives.**

— Internet security specialist, financial services

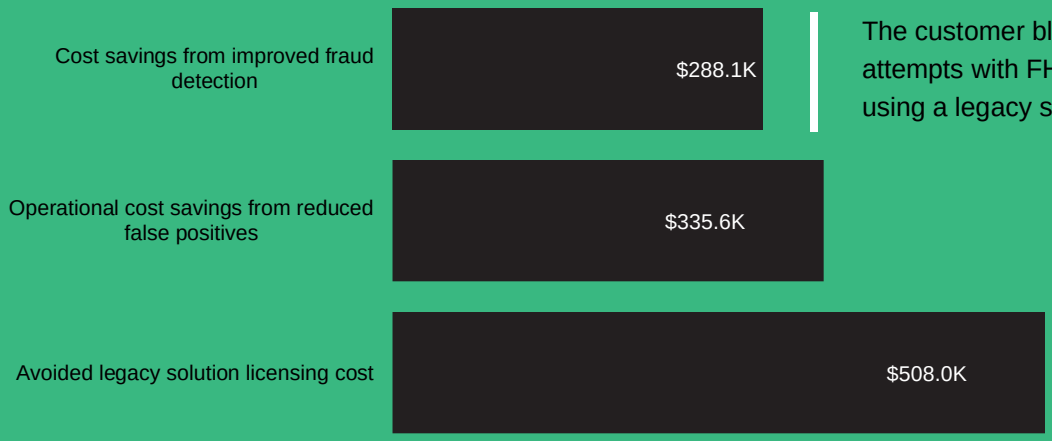
ROI
**130%**

BENEFITS PV
**$1.13M**

NPV
**$639K**

PAYBACK
**<6 months**

## Benefits (Three-Year)

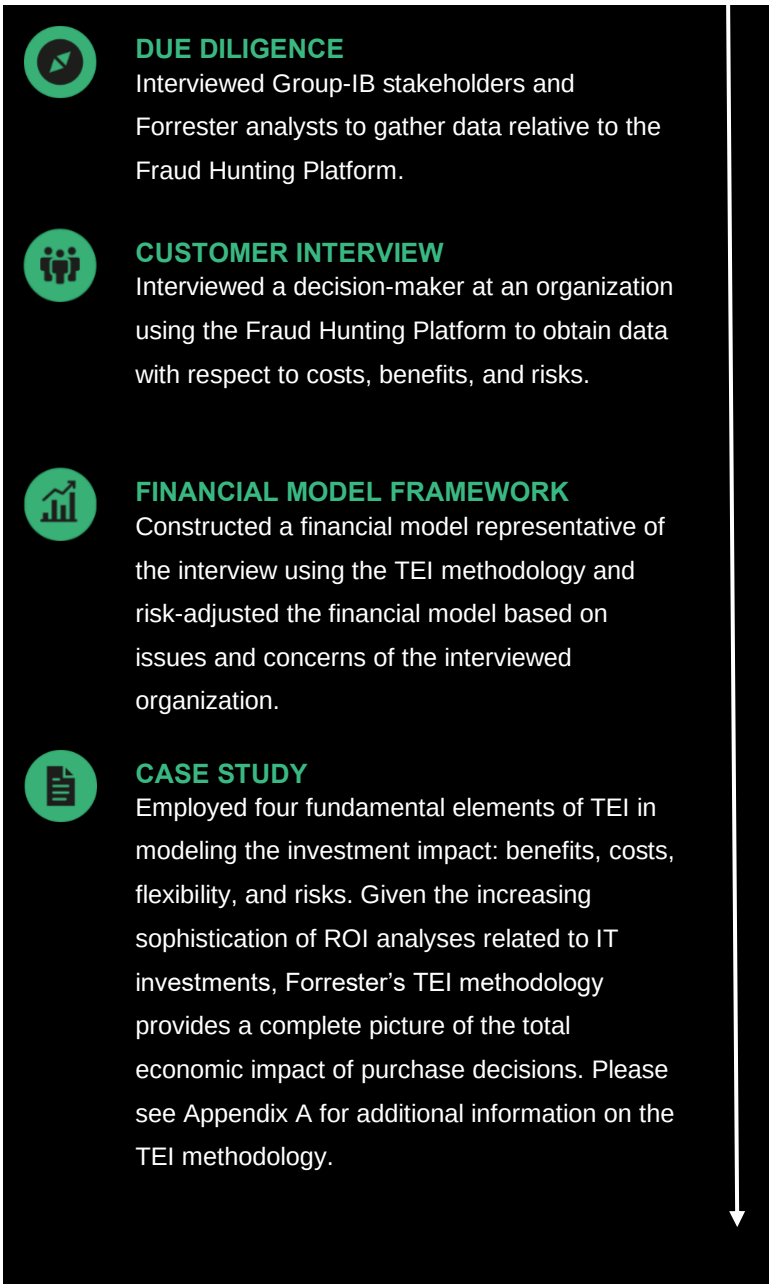



The customer blocked 70% to 80% of fraud attempts with FHP, an increase from 60% using a legacy solution.

## 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 Fraud Hunting Platform.

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 Fraud Hunting Platform can have on an organization.




**DISCLOSURES**

Readers should be aware of the following:

This study is commissioned by Group-IB 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 the Fraud Hunting Platform.

Group-IB 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.

Group-IB provided the customer name for the interview but did not participate in the interview.

# The Group-IB Fraud Hunting Platform Customer Journey

Drivers leading to the Fraud Hunting Platform investment

**INTERVIEWED ORGANIZATION**

Forrester interviewed a Group-IB Fraud Hunting Platform customer with the following characteristics:

- A financial services firm with 10 million online customers and over 6 million monthly online transactions. It generates $7 billion in annual revenue.
- Detected fraud with a legacy anti-fraud solution prior to using Fraud Hunting Platform.

**KEY CHALLENGES**

Customers of the organization were often the target of fraudsters using a diverse range of fraudulent activities including malware attacks, phishing, social engineering, and intimidation. As the organization tackled these fraud attempts, it struggled with common challenges, including:

- **Timely fraud detection and prevention.** The organization flagged a high number of transactions as false positives, which hindered employees from focusing on the actual risky transaction. As a result, it could not prevent all fraud attacks in time, and sometimes only found out about attacks when customers complained.
- **Meeting local regulations on cloud hosting.** The organization required cloud services hosted within the country and its legacy solution did not meet that requirement.

**USE CASE DESCRIPTION**

The regional financial services firm switched from a legacy anti-fraud software to Group-IB Fraud Hunting to detect and prevent fraud on its online banking portals.

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

**Key metrics**

- **10 million online customers**
- **Over 6 million monthly transactions**
- **Switches from a legacy anti-fraud solution**
- **Deploys Fraud Hunting Platform on its web portal**

**"Sometimes there are too many false positives, so our operators can't reach the customer on time or some fraudsters know the operations, so they somehow forward the calls from the banks, so we can't reach the customer."**
*Internet security specialist, financial services*

# Analysis Of Benefits

Quantified benefit data

## Total Benefits

| Ref. | Benefit | Year 1 | Year 2 | Year 3 | Total | Present Value |
|---|---|---|---|---|---|---|
| Atr | Improved fraud detection | $76,205 | $117,777 | $161,663 | $355,645 | $288,073 |
| Btr | Operational cost savings from reduced false positives | $109,224 | $136,664 | $164,162 | $410,049 | $335,577 |
| Ctr | Avoided legacy solution licensing cost | $195,000 | $204,750 | $214,988 | $614,738 | $508,011 |
| | Total benefits (risk-adjusted) | $380,429 | $459,191 | $540,813 | $1,380,432 | $1,131,661 |

### IMPROVED FRAUD DETECTION

**Evidence and data.** The organization prevented up to 80% of fraudulent attempts and mitigate the financial impact associated with successful attacks.

- The organization identified malicious software attacks, phishing, social engineering, and intimidation as the common tactics that fraudsters used on its customers. There were a few hundred of such attempts every year.
- Every time a customer fell victim to fraudsters, the organization incurred labor cost. The fraud team spent at least an hour investigating the cause and conducted deeper analysis if needed to prevent repeated attempts. Customer service representatives contacted the customer to explain what happened and guide them to reporting the attack to an authority.
- The organization also incurred costs in legal proceedings and reimbursements, as some customers would pursue compensation in court. The interviewee estimated that a smaller group of customers (10%) would be reimbursed.
- The interviewee also expected fines for incompliance, as regulations would take effect in the country it operated in imminently, requiring banks to monitor all online transactions.

**Modeling and assumptions.** Forrester makes the following assumptions for the financial model:

- Fraudsters attempt 560 attacks in Year 1. The number of attempts increases by 3% year-on-year with 577 in Year 2 and 594 in Year 3.
- Before using Fraud Hunting Platform, the organization manages to block 60% of attempts.
- With Fraud Hunting Platform, the organization detects and prevents more attacks: 70% in Year 1, gradually increasing to 80% as it collects more data and builds a fuller picture of normal versus abnormal user behavior.
- Average loss the organization incurs from a fraud incident is $400.
- Every dollar lost in fraud costs a financial organization $3.78.[1]

Fraud attempts FHP blocked

**70 to 80% over the three-year period**

**Risks.** Benefits from improved fraud detection may vary, depending on the following factors:

- The number of fraud attempts.
- The organization's ability to block fraud attempts prior to using FHP. This may vary depending on skills and knowledge of the fraud team, fraud prevention processes, and any solutions used (see side bar).
- The percentage of attempts the organization blocks prior to using Fraud Hunting Platform.
- Average fraud value and the cost to the organization.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $288,073.

## Fraud Detection Abilities Prior To Using FHP Vary

This study models the impact FHP has on fraud detection for a customer that previously used a commercial anti-fraud solution. While financial services and retail/e-commerce firms have invested the most in enterprise fraud management, individual organizations may differ in terms of the maturity of their anti-fraud practices.[2] For example, the organization might only block a smaller proportion of fraud attempts than 60% as modeled in row A2 below, if they rely on tools built inhouse or — in rare cases — if it battles fraud with manual transaction reviews only. These organizations can expect higher incremental improvements in fraud detection using FHP.

**Improved Fraud Detection**

| Ref. | Metric | Calculation | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| A1 | Fraud attempts | Interview | 560 | 577 | 594 |
| A2 | Percent of attempts blocked pre-FHP (using a legacy solution) | Assumption | 60% | 60% | 60% |
| A3 | Percent of attempts blocked with FHP | Interview | 70% | 75% | 80% |
| A4 | Average fraud value | Assumption | $400 | $400 | $400 |
| A5 | Cost to the bank per $1 fraud | External source | $3.78 | $3.78 | $3.78 |
| At | Improved fraud detection | A1*(A3-A2)*A4*A5 | $84,672 | $130,864 | $179,626 |
| | Risk adjustment | ↓10% | | | |
| Atr | Improved fraud detection (risk-adjusted) | | $76,205 | $117,777 | $161,663 |
| | **Three-year total: $355,645** | | **Three-year present value: $288,073** | | |

### OPERATIONAL COST SAVINGS FROM REDUCED FALSE POSITIVES

**Evidence and data.** Fraud Hunting Platform collects user and device data to enable the organization to detect anomalies in user behavior with a higher degree of confidence. This improved the accuracy of fraud detection, resulting in fewer false positives.

- Before using Fraud Hunting Platform, the interviewee's organization estimated that roughly 9% of transactions were flagged as false positives.
- In the first year of implementing the solution, the organization reduced false positives by 20%. The interviewee expected further reductions as the organization continued to establish user behavior and reduce collusion.

**"Because we established the customer's behavior, I can think it's less risky and focus on the riskier transaction … We collect data from the browser and whatever they can from the user's computer and [Group-IB] creates a unique number for that particular device. After some time, I can be confident that the same ID keeps coming with your transaction."**
*Internet security specialist, financial services*

**Modeling and assumptions.** Forrester makes the following assumptions:

- Without Fraud Hunting Platform, the organization flags 6.6 million transactions as false positives in Year 1, a number that increases by 3% every year with business growth.
- Fraud Hunting Platform reduces false positives by 20% in Year 1. Overtime the organization achieves a 30% reduction as it collects more data to better distinguish normal user and device behavior from potentially fraudulent ones.
- Fifteen call center operators and eight fraud analysts are relieved of the workload investigating and reaching out to customers for verification.
- Reducing false positive cases also means the organization sends fewer SMSs for two-factor authentication (2FA) purposes. About 30% of false positives require 2FA verification, costing $0.01.

**Risks.** Operational cost savings may vary, depending on the following factors:

- The number of flagged transactions that turn out to be false positives.
- The number of employees dedicated to investigating false positives and their salary, which varies based on a number of factors including seniority and location.
- The proportion of false positives that require SMS verification and the cost of sending SMS messages.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $335,577.

## Operational Cost Savings From Reduced False Positives

| Ref. | Metric | Calculation | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| B1 | Number of false positives | Y1: Assumption<br>Y2 and Y3: 3% YoY growth | 6,600,000 | 6,798,000 | 7,001,940 |
| B2 | Reduction in false positives | Interview | 20% | 25% | 30% |
| B3 | Number of call center operators | Interview | 15 | 15 | 15 |
| B4 | Average fully burdened salary | Assumption | $42,000 | $42,000 | $42,000 |
| B5 | Number of fraud analysts | Interview | 8 | 8 | 8 |
| B6 | Average fully burdened salary | Assumption | $68,000 | $68,000 | $68,000 |
| B7 | Productivity capture | Assumption | 50% | 50% | 50% |
| B8 | Percent of false positives that require 2FA via SMS | Interview | 30% | 30% | 30% |
| B9 | Cost per SMS | Assumption | $0.01 | $0.01 | $0.01 |
| Bt | Operational cost savings from reduced false positives | (B2*(B3*B4+B5*B6)*B7)+(B1*B2*B8*B9) | $121,360 | $151,849 | $182,402 |
| | Risk adjustment | ↓10% | | | |
| Btr | Operational cost savings from reduced false positives (risk-adjusted) | | $109,224 | $136,664 | $164,162 |
| | **Three-year total: $410,049** | | **Three-year present value: $335,577** | | |

### AVOIDED LEGACY SOLUTION LICENSING COST

**Evidence and data.** When the interviewee's organization switched to Fraud Hunting Platform, it avoided paying licensing fees for its legacy transactional anti-fraud solution, which cost 30% more than FHP.

**Modeling and assumptions.** Forrester makes the following assumptions:

- The organization avoids paying nearly $217k in licensing cost for their legacy anti-fraud solution in Year 1.
- The legacy solution licensing cost is assumed to increase 5% year-on-year, meaning the organization saves nearly $228K in Year 2 and nearly $239k in Year 3.
- Note the aforementioned amounts only account for the avoided legacy solution licensing cost. The organization pays licensing fees for Fraud Hunting Platform, detailed in the Cost section below.

**Risks.** The avoided legacy solution licensing costs may vary, depending on the legacy solution adopted and its pricing structure.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $508,011.

**Avoided Legacy Solution Licensing Cost**

| Ref. | Metric | Calculation | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| C1 | Legacy solution licensing cost | Y1: Composite<br>Y2 and Y3:5% YoY growth | $216,667 | $227,500 | $238,875 |
| Ct | Avoided legacy solution licensing cost | C1 | $216,667 | $227,500 | $238,875 |
| | Risk adjustment | ↓10% | | | |
| Ctr | Avoided legacy solution licensing cost (risk-adjusted) | | $195,000 | $204,750 | $214,988 |
| | **Three-year total: $614,738** | | **Three-year present value: $508,011** | | |

## UNQUANTIFIED BENEFITS

Additional benefits that the customer experienced but was not able to quantify include:

- **Improved customer experience.** Fraud Hunting Platform helps organization ensure security without creating friction. Organizations can whitelist customers based on insights the solution captures and eliminate the need for additional security control (e.g., complex passwords, 2FA). This improves customer experience.
- **Mitigated reputation risk by maintaining customer trust.** Minimizing the number of fraud cases helps build customer trust. The interviewed internet security specialist said, “If people start thinking that online banking at our bank is risky and they may get frauded, it is a very high cost." The executive added that consumer confidence that their assets are safe at the bank is essential to the bank’s reputation and customer retention and acquisition.

## FLEXIBILITY

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

- **Using Fraud Hunting Platform to prevent fraud on mobile channels.** Organizations can implement Fraud Hunting Platform on mobile applications. This protects mobile transactions against fraud and provides cybersecurity teams with additional user behavioral and device parameters to detect cross-channel fraud and uncover accounts that are accessed from known fraudulent devices.
- **Protecting a wider range of transactions and business activities.** Organizations can also use Fraud Hunting Platform to protect 3D Secure (3DS) pages from card-not-present fraud and block bad bot activities. It can also leverage the data collected to support anti-money laundering investigations and customer onboarding processes.

# Analysis Of Costs

Quantified cost data

| Total Costs | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Ref.** | **Cost** | **Initial** | **Year 1** | **Year 2** | **Year 3** | **Total** | **Present Value** |
| Dtr | Fraud Hunting Platform licensing cost | $0 | $175,000 | $175,000 | $183,750 | $533,750 | $441,773 |
| Etr | Implementation and ongoing running cost | $45,025 | $2,423 | $2,423 | $2,423 | $52,294 | $51,051 |
| | Total costs (risk-adjusted) | $45,025 | $177,423 | $177,423 | $186,173 | $586,044 | $492,824 |

### FRAUD HUNTING PLATFORM LICENSING COST

**Evidence and data.** Fraud Hunting Platform is priced based on the number of unique users (customers) and the channels covered (web and mobile). Clients may also opt in to additional modules such as the Preventive Proxy for a premium.

**Modeling and assumptions.** Forrester makes the following assumptions for the organization:

- The organization uses Fraud Hunting Platform on its online banking portal, which services 10 million customers.
- It signs a two-year contract with Group-IB and pays just over $167K in Year 1 and Year 2.
- After a two-year contract, the licensing costs increases by 5% to $175k to align with business growth.

**Risks.** The licensing cost may vary, depending on the number of customers an organization has, whether it uses the solution on web portals and/or mobile apps, and whether it opts in for additional modules/services.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $441,773.

| Fraud Hunting Platform Licensing Cost | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Calculation** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| D1 | Annual licensing cost | | | $166,667 | $166,667 | $175,000 |
| Dt | Fraud Hunting Platform licensing cost | D1 | $0 | $166,667 | $166,667 | $175,000 |
| | Risk adjustment | ↑5% | | | | |
| Dtr | Fraud Hunting Platform licensing cost (risk-adjusted) | | $0 | $175,000 | $175,000 | $183,750 |
| | **Three-year total: $533,750** | | | **Three-year present value: $441,773** | | |

## IMPLEMENTATION AND ONGOING RUNNING COST

**Evidence and data.** The implementation of Fraud Hunting Platform is a collaboration between the client and Group-IB. Stakeholders from fraud/cybersecurity and developers from the customer organization work with Group-IB to gather data requirements for the solution, implement and integrate the solution with the client's internal systems and third-party solutions, and conduct testing before the solution goes into production.

- The interviewee's organization spent three months implementing Fraud Hunting Platform. Internally, one developer took on most of the hands-on work and spent 20% of their time on the implementation and two to three business stakeholders participated in meetings.
    - The interviewee commented on the benefit of deploying the solution on cloud: "The more difficult part in such projects is not implementing code, but whether it works on your data infrastructure — all the networking, traffic, firewall mostly. So, since it's in the cloud, it was very simple for us."
- A team of fraud analysts underwent a one-day training before they started using Fraud Hunting Platform to learn about its features and how to leverage insights it generated to tackle fraud.
- Ongoing management of Fraud Hunting Platform involves maintaining integrations between the solution and the organization's core systems and other third-party software.

**Modeling and assumptions.** Forrester makes the following assumptions about the organization:

- The organization pays Group-IB a one-off fee of $35,000 for professional services for the implementation.
- The organization dedicated 120 hours of internal effort on the implementation over three months. This includes a developer spending 20% of their time a year (104 hours) and two business stakeholders with some seniority each spending 8 hours in meetings, totaling 16 hours.
- The organization trains eight fraud analysts to use Fraud Hunting Platform.

**Risks.** The implementation and ongoing management cost may vary, depending on the follow factors:

- The complexity of the organization's IT environment and the number of modules being implemented.
- The number of employees involved in implementation and ongoing management, as well as their seniority.
- The organization's maturity in terms of fraud prevention, and the level of technical skills and knowledge that its employees possess.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $51,051.

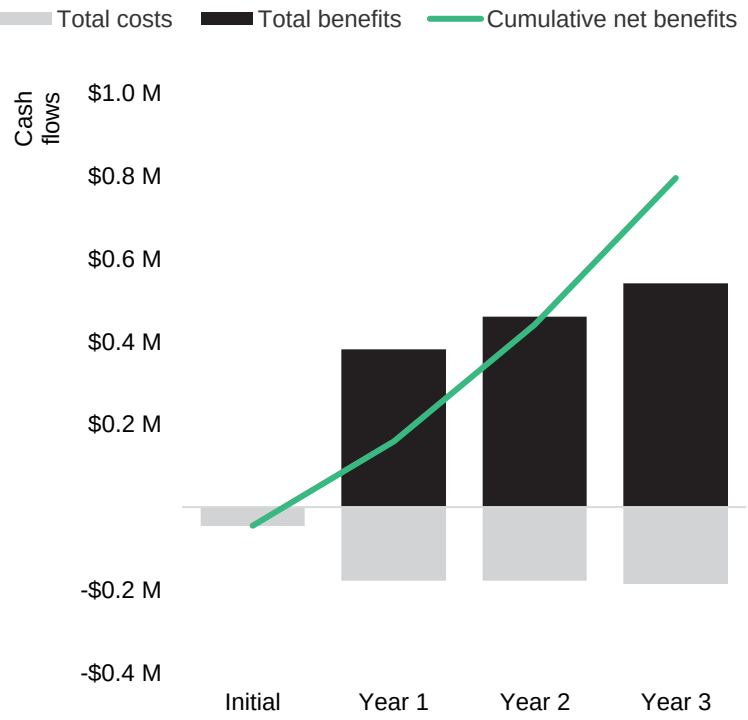
## Implementation And Ongoing Running Cost

| Ref. | Metric | Calculation | Initial | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|---|
| E1 | Professional services cost | | $35,000 | | | |
| E2 | Internal hours spent | | 120 | 48 | 48 | 48 |
| E3 | Average fully burdened salary (internal project team) | | $100,000 | $100,000 | $100,000 | $100,000 |
| E4 | Internal effort | E2*E3/2,080 | $5,769 | $2,308 | $2,308 | $2,308 |
| E5 | Number of fraud analysts | | 8 | | | |
| E6 | Training time (hours) | | 8 | | | |
| E7 | Fraud analyst average fully burdened salary | $68,000/2,080 | $33 | | | |
| Et | Implementation and ongoing running cost | (E1+E4)+(E5*E6*E7) | $42,881 | $2,308 | $2,308 | $2,308 |
| | Risk adjustment | ↑5% | | | | |
| Etr | Implementation and ongoing running cost (risk-adjusted) | | $45,025 | $2,423 | $2,423 | $2,423 |
| | **Three-year total: $52,294** | | **Three-year present value: $51,051** | | | |

# Financial Summary

## CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

### Cash Flow Chart (Risk-Adjusted)




The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite 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 | ($45,025) | ($177,423) | ($177,423) | ($186,173) | ($586,044) | ($492,824) |
| Total benefits | $0 | $380,429 | $459,191 | $540,813 | $1,380,432 | $1,131,661 |
| Net benefits | ($45,025) | $203,006 | $281,768 | $354,639 | $794,388 | $638,837 |
| ROI | | | | | | 130% |
| 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: Supplemental Material

*Related Forrester Research*

"Top Enterprise Fraud Management And Anti-Money Laundering Trends," Forrester Research, Inc., December 17, 2018.

"The Top Trends Shaping Anti-Money Laundering In 2020," Forrester Research, Inc., August 10, 2020.

## Appendix C: Endnotes

[1] "Transform Your Strategy To Safely Navigate The Rising Risk Of Fraud." LexisNexis Risk Solutions, 2020.
[2] The Worldwide Annual EFM Market Is Set To Grow To $7.58 Billion In 2025," Forrester (https://www.forrester.com/fn/4xm8SHJqv1nNCwr6lEDS9X).


FORRESTER®