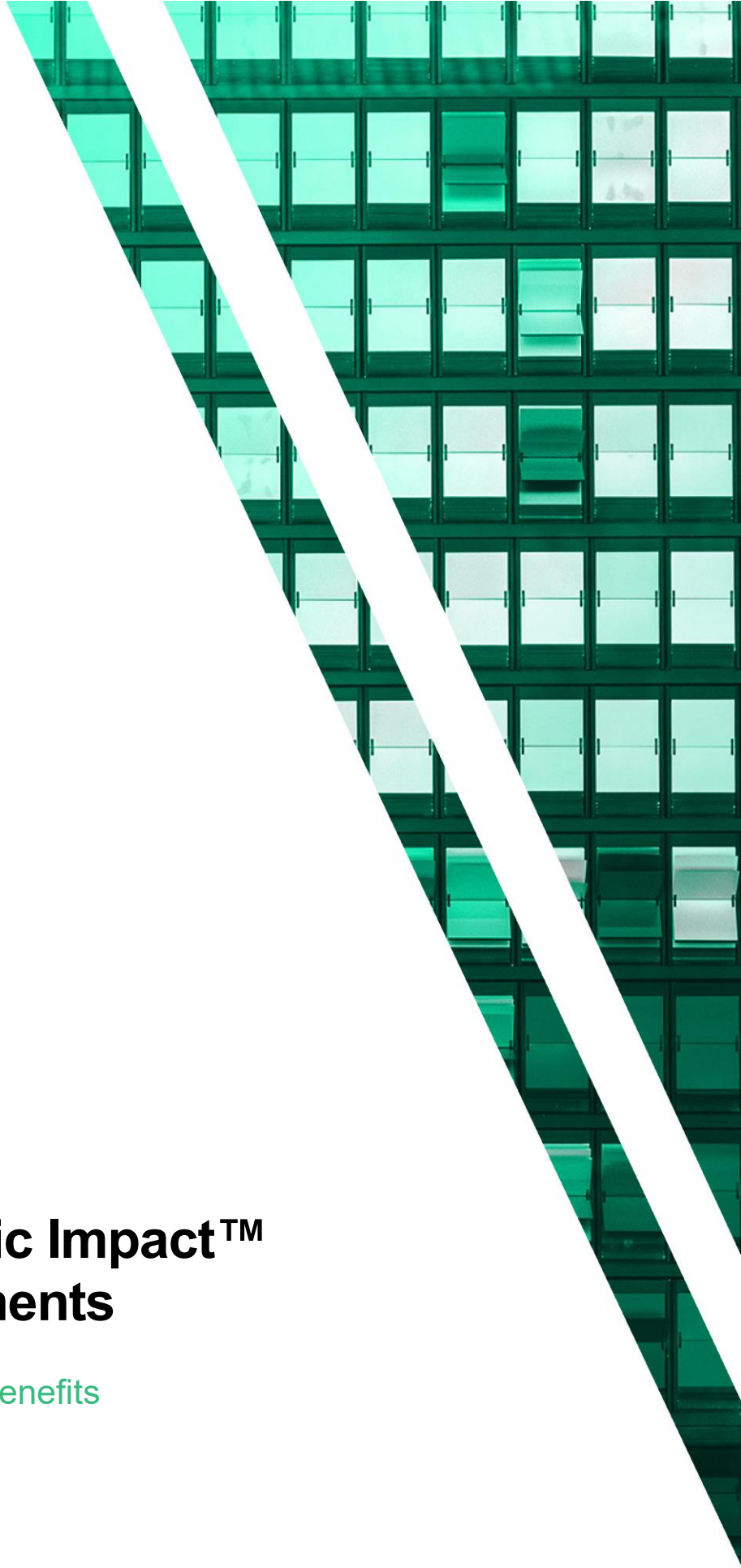
FORRESTER®



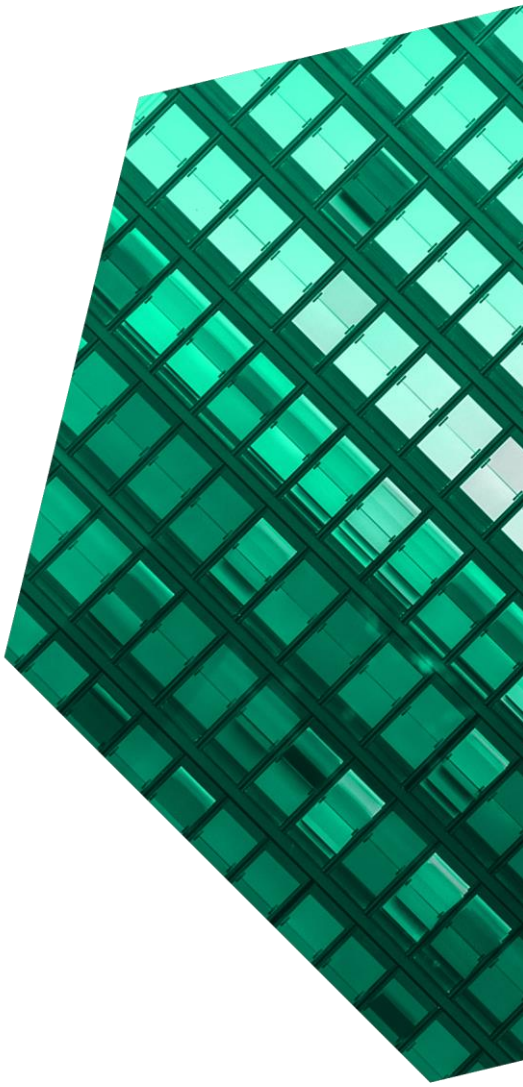
The Total Economic Impact™ Of IBM Safer Payments

Cost Savings And Business Benefits Enabled By Safer Payments

JANUARY 2021

Table Of Contents

Consulting Team: Veronica Iles
Luca Son



Executive Summary

The introduction of real-time payments, new types of financial services products, and disruptive technologies has fostered an environment ripe for bad-actor exploitation. Organizations using IBM Safer Payments can harness machine learning to improve fraud management performance, minimize fraud losses, reduce false-positive rates, lower the costs of investigation, and overcome the limitations of legacy fraud management methods, saving millions of dollars without hampering genuine activity.

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

Fraud and payments have been intertwined since the early days of bartering. The evolution of financial instruments and the emergence of new payment channels and vendors have presented bad actors with new avenues to commit fraud and evolved the fraud prevention market.

Professionals specializing in antifraud are increasingly challenged to develop new behavioral patterns and models to detect cybercriminal activity across a wide variety of payment channels. Many turn to IBM Safer Payments to provide real-time fraud prevention for all cashless payment systems. With IBM Safer Payments, organizations can leverage machine learning capabilities and deploy new models to combat the increasing volume and complexity of fraud attacks.

The IBM Safer Payments solution builds upon an organization's legacy statistical models by adding direct detection features as it evaluates financial institution-specific transactions. The solution uses AI capabilities to evaluate current rules used to detect fraud as well as suggest new or enhanced rules, validate them, and implement them within days. The system can even identify new, emerging fraud trends. AI generates recommendations for human analysts to improve rule sets and test suggestions without interrupting production; analysts can then choose whether to include the recommendation. IBM Safer Payments also creates a profile per person or per merchant, and the system looks across channels for similar transactions, creating contacts between people and a more robust view of the transactor.

KEY STATISTICS

Return on investment (ROI)
144%

Net present value (NPV)
$10.0M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five customers with experience using IBM Safer Payments. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite organization.

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include the following, modeled by the composite organization:

- **Better fraud detection results in avoided fraud losses of $13.0 million.** The improved performance and scale of IBM Safer Payments over rules-based methods result in the reduction of basis points lost to fraud in both the digital and card channels. Over three years and a cumulative total of 800 million transactions annually, the avoided fraud losses are worth more than $13.0 million to the organization.
- **Improved model accuracy reduces false-positive rates by up to 77% and improves analyst productivity.** IBM Safer Payments models improve accuracy based on transactional data, navigational data, and analyst decisions, culminating in lower false-positive rates and providing analysts with the information necessary to evaluate transactions more efficiently. Over three years and a cumulative total of nearly 90,000 avoided analyst review hours, the improvements are worth more than $2.7 million to the organization.
- **The organization avoids $1.0 million in one-time legacy system upgrades and $230K annually for ongoing licensing costs.** The legacy rules-based systems are high-maintenance, requiring costly tuning and annual updates. Over three years, the organization saves $1.3 million by avoiding upgrades and licensing costs.

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

- The creation of a new revenue channel by offering IBM Safer Payments as a service to clients.
- Savings through reliance on business units rather than outside vendors or consultants.
- The ability to increase the frequency and speed of model changes.
- Decreased transaction friction and in-tact customer experience due to faster risk scoring (in milliseconds).
- Improved employee experience with user-friendly UX that makes necessary information available in one location.
- Extended solution effectiveness due to evolution with an open environment, resulting in a longer-term investment.
- Deeper relationships with clients by collaborating and offering controlled access to rule sets.

Costs. Risk-adjusted PV costs include the following, modeled by the composite organization:

- **Internal costs include implementation labor over eight months and supporting hardware costs totaling $356K.** Hardware purchases and dedicated internal business and technical resources support the implementation over the course of eight months, costing $356K to the organization.
- **Payments made to IBM include three-year IBM licensing, support, and implementation consulting cost, totaling $5.4 million.** External costs include annual licensing costs covering 800 million annual transactions and a one-time fee of $600K for implementation consulting services.
- **An operations manager and analysts provide ongoing tuning and optimization of IBM Safer Payments, totaling $1.2 million.** Internal labor costs include one operations manager and up to five analysts. The ongoing costs total $1.2 million to the organization.

The customer interviews and financial analysis found that a composite organization experiences benefits of $17.0 million over three years versus costs of $7.0 million, adding up to a net present value (NPV) of $10.0 million and an ROI of 144%.

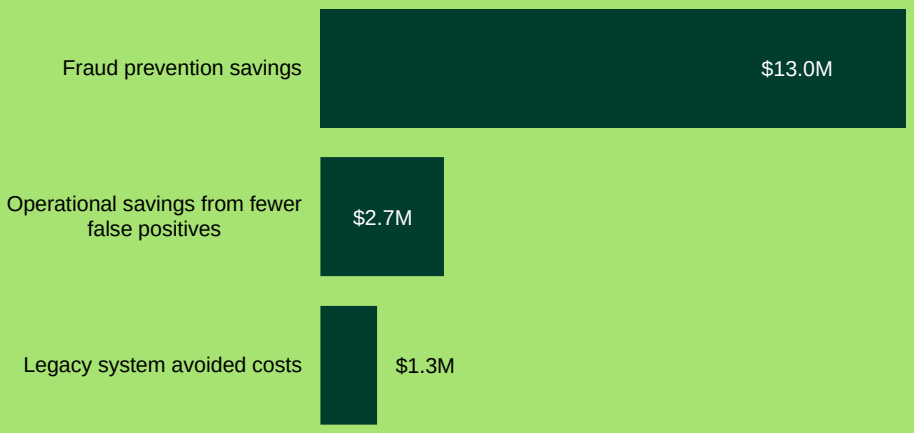
ROI
144%

BENEFITS PV
$17.0M

NPV
$10.0M

PAYBACK
<6 months

Benefits (Three-Year)



“The beauty of Safer Payments is the confidence that we have in the rules and the models and the ability to detect fraud very, very fast with low false positives.”

— Chief security officer, banking

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 IBM Safer Payments.

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 the IBM Safer Payments can have on an organization.

DUE DILIGENCE

Interviewed IBM stakeholders and Forrester analysts to gather data relative to IBM Safer Payments.

CUSTOMER INTERVIEWS

Interviewed five decision-makers at organizations using IBM Safer Payments to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewed organizations.

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 interviewed organizations.

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.

The IBM Safer Payments Customer Journey

Drivers leading to the Safer Payments investment

Interviewed Organizations

Industry	Interviewee(s)	Region	Busines Characteristics
Clearing and card services	Risk-scoring manager	Europe	$106 million in revenue 160 employees
Fraud detection as a service	Director of payments	US	$9 billion in revenue 10,000 employees
Financial services	SVP of digital payments Director of fraud and analytics	US	$12 billion in revenue 55,000 employees
Banking	Chief security officer	APAC	$6 billion in revenue 5,000 employees
Payments service provider	Director of fraud prevention	Europe	Undisclosed revenue 1,000 employees

KEY CHALLENGES

Before turning to IBM Safer Payments, the interviewed organizations relied on complex fraud detection technology stacks that combined in-house custom solutions and third-party fraud prevention tools. These solutions generated several pain points for the customers:

- **Legacy solutions lacked real-time decline capabilities.** With the appearance and wide adoption of real-time transactions, payment processors and banks needed to evaluate risk and make decisions in milliseconds. Batch-processed environments, however, made this crucial functionally impossible. The director of fraud and analytics shared: “In our previous solution, we did not have the ability to actually decline in real time. It was really the biggest motivator towards changing systems.”
- **Legacy solutions were siloed between payment channel, geographic region, or business unit, providing only a limited picture of human behavior.** Legacy solutions typically evaluated one type of channel but lacked the breadth to evaluate across all payment channels. Customers needed a tool that provided a more encompassing view of behavior across payment channels.

> **“With a batch environment processing real-time payments, I would receive an update that this could be fraud, but that payment is already gone. So we might be able to stop other payments, but that wasn’t easy because the model was based on a rule set that we couldn’t adjust for individual clients.”**
>
> *SVP of digital payments, financial services*

- **Incumbent vendors used black-box models, leaving customers in the dark as to why decisions were made.** When relying on a third-party fraud tool, customers had little to no control over model creation or rule development. The SVP of digital payments shared: **“**In our previous environment, we were at their mercy. We only could say, ‘We have an issue,’ but when we tried

to work with them, their answer always was, 'This is proprietary.'"

- **Legacy fraud prevention models were based on historical data and difficult to update.** The world of payments is continuously evolving, with new data sources, new products, and a movement toward increasingly digital and faster payments. In that landscape, the legacy systems that had been in place for many years were difficult to change. As patterns evolved, the legacy systems made noise, blocking transactions and missing the actual fraud until the fraud scales and statistical models were updated.

> **"Ours is a business where you have to stay ahead of the fraudsters. Our legacy fraud detection solutions couldn't keep up with the demands of newer fraud types, the speed at which transactions are changing, the volume of transactions, and the type of card products out there. So the biggest challenge with the legacy solution was it lacked the sophistication needed to keep up with new fraud patterns."**
>
> *Director of payments, fraud detection as a service*

WHY IBM?

Organizations typically select and stay with a fraud prevention solution for decades because shifting to a new vendor is like undergoing a heart and lung transplant. Due to this challenge, organizations only switch when they absolutely must. Customers evaluated multiple fraud-detection vendors by conducting requests for proposal (RFPs), proofs of concept (PoCs), and business-case process evaluations. Interviewees cited the following reasons for choosing IBM Safer Payments:

- **IBM Safer Payments offers agility and scale to react to new fraud patterns in days rather than months.** Tired of falling behind bad actors, customers needed a tool that could adapt as quickly as new fraud trends emerge. **"** … [W]e wanted the solution to be sophisticated enough to look out for new, emerging trends. We found that IBM fit that criteria because the software would detect patterns based on previous historical trends and apply to new trends. Based on the proof of concept, that was a significant improvement from our in-house solution."

> **"Safer Payments was by far the fastest, high-performing tool, and we were able to risk-score extremely quickly, so the customer experience would not in any way be tarnished, and plus, we also want speed for other reasons, obviously."**
>
> *Chief security officer, banking*

- **IBM Safer Payments is a modern open data science platform that can consume externally developed models.** As opposed to legacy solutions that use statistical modeling of large data sets, IBM uses artificial intelligence to dynamically adapt to new data. Eager to move to a next-generation approach with visibility into the fraud models, the SVP of digital payments shared: "IBM's solution offered the opportunity to move away from a proprietary black box. We went from 'I can't tell you what we're doing with your rules' to IBM allowing us to rewrite and create our own rules and play with those in a sandbox before we ever turn them live. It was just so appealing for us."

"What stood out with IBM was that it had the most advanced AI capability built in, which plays a key component in the ability for the tool to stay relevant."

Chief security officer, banking

- **IBM is a long-established mature technology firm with an international presence and consulting abilities for all customers.** With such a major investment, customers noted that it was important to have a vendor that could provide support anywhere in the world. The director of payments shared: "We chose IBM because of the sophistication of the platform and the implementation team. In my experience of having worked with vendors and partners in the financial services industry, if you don't have the right integration and the right customer service support, you might as well just be in-house."
- **Simple user experience (UX) and IT-agnostic transparent models enabled business unit ownership and adoption of the tool.** The IBM Safer Payments solution is designed to be IT agnostic. The tool provides transparency into why a transaction is denied, so customers can directly improve the models without engaging IT or a third party. The chief security officer shared, "One reasons we picked IBM Safer Payments was the ability for us to self-manage, self-soothe that tool, right at the financial crime management center level, so we don't have to default to IBM every time that we want to make changes."
- **The enterprise tool provided a multi- and cross-channel perspective and could quickly scale to handle real-time payments and emerging trends.** Customers noted that it was no longer enough to look at transaction behavior through a single channel lens. Within IBM Safer Payments' flexible data model, the behavioral analysis tool uses machine learning and AI to scrutinize behavior across payment channels, including credit cards, ATMs, online banking, and newer digital and real-time payment channels. The director of payments shared: "Our first decision-making criterion was that we should be able to run the entire portfolio through the solution. We wanted to make sure that it wasn't just a subset of payments."

"IBM has given us so much more flexibility in writing rules. It is almost never a question as to if I can write a rule; there are usually three different ways to do it. It's a very flexible system, and that has been incredibly meaningful for us, especially in P2P [peer-to-peer] because the fraud is evolving and changing so quickly."

Director of fraud and analytics, financial services

- **Customers had the option to host IBM Safer Payments on-premises or in any cloud.** Customers appreciated the flexibility when deciding where to host the IBM Safer Payments tool. The chief security officer noted, "IBM Safer Payment's ability to be hosted in the cloud was attractive for us and is one of the beauties of their model."

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the five companies that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global, multibillion-dollar midsize bank evaluates fraud risk across 800 million transactions annually (500 million card transactions and 300 million digital transactions). The organization has 7,000 employees and a fraud team of 50.

Deployment characteristics. The organization has an on-premises deployment of IBM Safer Payments

Investment objectives. The composite organization has the following goals for its IBM Safer Payments investment:

- Have real-time risk scoring with low response times to reduce fraud without hampering legitimate activity.
- Adapt quickly to new fraud and payment types.

Key assumptions

- **Midsize bank**
- **$5 billion in revenue**
- **7,000 employees**
- **50 fraud analysts**
- **800 million transactions annually**

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Fraud prevention savings	$4,752,000	$5,256,000	$5,774,400	$15,782,400	$13,002,194
Btr	Operational savings from fewer false positives	$1,062,720	$1,102,904	$1,152,830	$3,318,454	$2,743,738
Ctr	Legacy system avoided costs	$1,045,500	$195,500	$195,500	$1,436,500	$1,258,907
	Total benefits (risk-adjusted)	$6,860,220	$6,554,404	$7,122,730	$20,537,354	$17,004,839

FRAUD PREVENTION SAVINGS

The primary objective customers cited for adopting IBM Safer payments was to minimize fraud losses while maintaining a frictionless customer experience. The interviewees' organizations measured their success in several ways:

- The risk-scoring manager shared that his organization was able to increase its fraud detection rate by 2x, allowing the company to save millions of dollars without hampering genuine activity.

"With Safer Payments, we can be more surgical in how we respond, what we turn off, how we block the card or don't block the card, the timeframes, geographical locations, whatever it might be. The customer experience will be enhanced, and the inconvenience will be reduced. And when we do need to take steps, we can do so in a more surgical manner."

Chief security officer, banking

- The SVP of digital payments shared: "Overall, our fraud rate has gone down tremendously. We've had customers in a P2P network that haven't recorded fraud since they've gone live. We have over half of our customers that had not reported fraud in the P2P space, and we reduced our attempted fraud down to 97%. So we have about a 3% rate of attempted fraud on our client base."

Modeling and assumptions. To capture the interviewees' experiences, Forrester assumes:

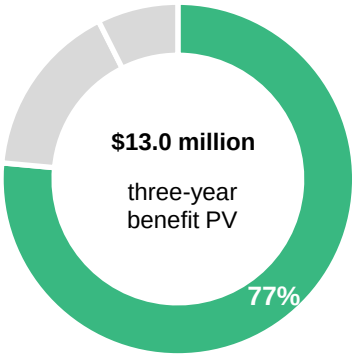
- The composite organization evaluates 500 million, 505 million, and 510 million credit card transactions in Years 1, 2, and 3, respectively.
- The average order value for a card transaction is $30.
- In the prior environment, the composite organization lost 4 basis points to fraud each year in its card channel.
- With the investment in Safer Payments, the average basis points lost to fraud in the card channel decrease to 2.
- The composite organization evaluates 300 million, 305 million, and 310 million digital transactions in Years 1, 2, and 3, respectively.

- The average order value for a digital transaction is $20.
- In the prior environment, the composite organization lost 25 basis points to fraud each year in its digital payments channel.
- With the investment in IBM Safer Payments, the average basis points lost to fraud in the digital payments channel decrease to 19 in Year 1. Each year, the basis points lost to fraud in the digital channel decrease by 1 as fraud detection rates improve.
- Eighty percent of the impact is attributed to the IBM Safer Payments investment; the remaining 20% is attributed to outside economic factors.

Risks. These results may not be representative of all experiences; fraud prevention savings will vary between organizations depending on numerous factors, including payment channel, transaction volumes, region, legacy environment status quo, and optimization of rules and models. Artificial intelligence and machine learning technologies are maturing, and improve risk scoring, predictive case investigation, and contextual reporting but require model governance and may have issues with error rates and precision and depend on training data availability and quality.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $13.0 million.

Fraud Prevention Savings



Fraud Prevention Savings

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
A1	Annual card transaction volume	Composite	500,000,000	505,000,000	510,000,000
A2	Average card order value	Composite	$30	$30	$30
A3	Basis points lost to fraud in legacy environment	Interviews	4	4	4
A4	Basis points lost to fraud with IBM Safer Payments	Interviews	2	2	2
A5	Avoided basis points	A3-A4	2	2	2
A6	Subtotal: Avoided card payment fraud losses	A1*A2*A5* 0.01%	$3,000,000	$3,030,000	$3,060,000
A7	Annual digital payment transaction volume	Composite	300,000,000	305,000,000	310,000,000
A8	Average digital payments order value	Composite	$20	$20	$20
A9	Basis points lost to fraud in legacy environment	Interviews	25	25	25
A10	Basis points lost to fraud with IBM Safer Payments	Interviews	19	18	17
A11	Avoided basis points	A9-A10	6	7	8
A12	Subtotal: Avoided digital payment fraud losses	A7*A8*A11 *.01%	$3,600,000	$4,270,000	$4,960,000
A13	Attribution to IBM Safer Payments	Assumption	80%	80%	80%
At	Fraud prevention savings	(A6+A12)*A13	$5,280,000	$5,840,000	$6,416,000
	Risk adjustment	↓10%			
Atr	Fraud prevention savings (risk-adjusted)		$4,752,000	$5,256,000	$5,774,400
	Three-year total: $15,782,400		**Three-year present value: $13,002,194**		

OPERATIONAL SAVINGS FROM FEWER FALSE POSITIVES

In the legacy environment, customers could not adapt their risk-scoring models or write new static rules quickly enough to stay abreast of evolving fraud methods, especially in emerging channels like digital payments. Major consequences of rules-based systems included high false positives or delays and negative impacts to the end customer.

IBM Safer Payments enabled customers to reduce the number of false positives flagged by their legacy environments and empowered human agents to review possible false positives more efficiently. The interviewed organizations measured their success in several ways:

- **Fewer false positives.** The director of fraud and analytics shared: "When we talk about a reduction in false positives, we're talking about transactions that alerted and ultimately are closed as genuine. It is a waste of time for my team. Since moving to IBM Safer Payments, we're measuring about a 73% improvement in false positives."
- **Significant reduction in the false positive ratio.** The chief security officer of a bank measured a significant improvement with IBM Safer Payments, sharing: "Most banks are quite keen if their false positives sit somewhere around a 1-to-15 to a 1-to-12 ratio. We had it down to 1 to 5 previously, and with IBM Safer Payments, it has come down to 1 to 1.5. You actually can't get any lower than that."
- **More efficient review of transactions by analysts.** The SVP of digital payments shared: "The goal before IBM Safer Payments was for our analysts to work at least 15 cases per hour. We've been able to increase that caseload for them to sometimes 20 to 30 per hour because we know that the cases coming through are legitimate fraud opportunities. Before, our false-positive rate was through the roof, and we had to scrub through the data."

"Now with the rules and the intelligence, it looks at the data across the organization. Our team is now working smarter because the alerts coming in are smarter. It's been a tremendous opportunity for the team to improve how they work and how they learn."

SVP of digital payments, financial services

"Our goal was to drive down as many false positives as possible, and the team has done a phenomenal job with that. So now our analysts can work real fraud cases. The false positives from our old provider were killing us."

SVP of digital payments, financial services

"One of the things that really attracted us to Safer Payments was the ability to use artificial intelligence to make a decision in milliseconds. We can either accept that decision or review that decision before it goes out."

SVP of digital payments, financial services

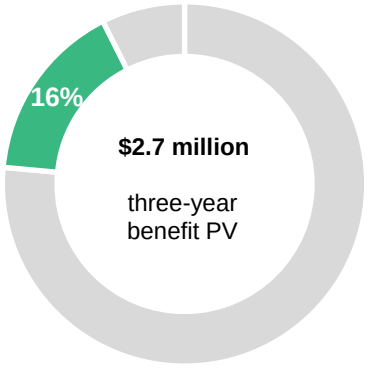
Modeling and assumptions. To capture the interviewees' implementation experiences, Forrester assumes:

- The composite organization has a transaction intercept rate of 0.03% across all payment channels, resulting in 240,000 to 246,000 transactions requiring analyst review.
- In the legacy environment, each transaction that was manually reviewed by an analyst took 9 minutes on average.
- With the investment in IBM Safer Payments, more sophisticated fraud models, and the multichannel evaluation of behavior, the number of transactions selected for human review decreases by 70%, 73%, and 77% in Years 1, 2, and 3, respectively.
- Analysts reviewing transactions in IBM Safer Payments have a single view of the customer, which allows investigation to include multi- and cross-channel information at their fingertips in a friendly UX, allowing them to review transactions more efficiently and reducing the average time to 6 minutes.
- The burdened hourly rate of an analyst is $41.

Risks. These results may not be representative of all experiences; the savings from fewer false positives and productivity lift of analysts will vary between organizations depending on the number of transactions reviewed, the burdened cost of analysts, and the ability for agents to more effectively review transactions using the information provided. Another factor to consider is the average size of transactions, which may alter the time necessary to review. The director of payments shared: "For larger-dollar transactions, there are more exceptions, which means you have to escalate it internally and have it reviewed. The process could take 24 hours to validate that transaction." Agents could potentially experience an even greater productivity lift than modeled here.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2.7 million.

Operational Savings From Fewer False Positives



Operational Savings From Fewer False Positives

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
B1	Number of alerts (all channels) in legacy environment	Intercept rate of 0.03%	240,000	243,000	246,000
B2	Average time for manual transaction review in legacy environment (minutes)	Interviews	9	9	9
B3	Subtotal: Number of hours of manual review in legacy environment	B1*B2/60 minutes	36,000	36,450	36,900
B4	Reduction in number of transactions selected for manual review	Interviews	70%	73%	77%
B5	Number of manual reviews in IBM environment	B1*(1-B4)	72,000	65,610	56,580
B6	Average time for manual transaction review in IBM environment (minutes)	1.5x faster than legacy environment	6	6	6
B7	Subtotal: Number of hours of manual review in IBM environment	B5*B6/60 minutes	7,200	6,561	5,658
B8	Number of transaction review hours avoided using IBM Safer Payments	B3-B7	28,800	29,889	31,242
B9	Hourly burdened cost of fraud analyst (rounded)	$85,000/2,080 hours	$41	$41	$41
Bt	Operational savings from fewer false positives	B8*B9	$1,180,800	$1,225,449	$1,280,922
	Risk adjustment	↓10%			
Btr	Operational savings from fewer false positives (risk-adjusted)		$1,062,720	$1,102,904	$1,152,830
	Three-year total: $3,318,454		**Three-year present value: $2,743,738**		

LEGACY SYSTEM AVOIDED COSTS

Legacy rules-based systems were high-maintenance, requiring costly tuning and annual updates. Data scientists to run the systems could be difficult to find and afford. The interviewed organizations realized savings in several categories measured against the legacy environment.

- **Fixed cost savings.** Customers were able to reduce spend related to ancillary technology investments, software upgrades, and additional purchases of hardware to support their legacy solutions. Customers noted a range of savings between $1 million and $5 million.
- **Variable cost savings.** Some of the previous solution vendors charged on a flat-pricing model, limiting the scalability of operations and inhibiting an enterprise fraud model.
- **Support and overhead.** The legacy environments were highly manual, and customers would have had to invest in additional fraud analysts, data scientists, and compute environment staff to continue to support it. Customers estimated that with IBM Safer Payments, they could avoid hiring between five and 15 additional headcounts.

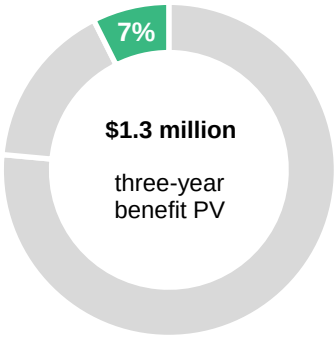
Modeling and assumptions. To capture the interviewees' implementation experiences, Forrester assumes:

- The composite organization avoids spending $1.0 million to upgrade its legacy fraud solution. This includes software and fraud model upgrades, additional headcount, and upgrading server hardware.
- The composite organization avoids $230,000 annually that it previously spent on the ongoing licensing costs related to legacy servers.

Risks. These results may not be representative of all experiences; the legacy environment savings will vary between organizations depending on legacy environment status quo, existing infrastructure, ability to retire legacy tools and hardware, and contract terms of with legacy solution provider. One customer was not able to realize legacy savings until the third year of investment because it was locked into a five-year contract with its legacy vendor.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1.3 million.

Legacy System Avoided Costs



Legacy System Avoided Costs

Ref.	Metric	Calculation	Year 1	Year 2	Year 3
C1	Avoided one-time payments for upgrading legacy fraud solution	Interviews	$1,000,000		
C2	Avoided licensing for legacy servers	Interviews	$230,000	$230,000	$230,000
Ct	Legacy system avoided costs	C1+C2	$1,230,000	$230,000	$230,000
	Risk adjustment	↓15%			
Ctr	Legacy system avoided costs (risk-adjusted)		$1,045,500	$195,500	$195,500
	Three-year total: $1,436,500		**Three-year present value: $1,258,907**		

UNQUANTIFIED BENEFITS

In addition to the three benefits quantified above, Forrester uncovered additional benefits that could not be quantified for this study but are nonetheless considered measurements of success for the IBM Safer Payments investment. These unquantified benefits include:

- **The creation of a new revenue channel.** Two of the interviewees described how their firms have been able to monetize IBM Safer Payments as a product offering. The SVP of digital payments shared: "We're able to sell the IBM product as a premium service to our clients and provide them with their own rule-writing capability, which has been a nice uptick for us. We've been able to create a new revenue stream with this offering where we're going to offer consulting services for financial institutions."
- **Professional services savings through reliance on business units rather than vendors.** In the legacy environments, customers had to wait for vendors to update models or engage additional services to make ad hoc changes. The chief security officer said: "Every time we want to make changes, the user can do it directly. That makes it very cost-effective and adaptive. We have a dynamic threat environment, so we need to be able to respond and adapt quickly. That's definitely a key benefit for us in Safer Payments."
- **The ability to increase the frequency and speed of model changes.** The benefits above could not have been realized without the speed and flexibility provided by IBM Safer Payments when it comes to creating and adapting fraud models. The director of fraud said: "The flexibility in the IBM Safer Payments system is really impactful. We must make real-time adaptations and changes as quickly as possible. So my analytics team makes changes to the rule set probably two to three times a week. It was absolutely impossible for us to do that before." IBM Safer Payments drastically reduces model update cycle times, allowing analysts to make changes frequently, which improves fraud detection and minimizes losses between update cycles.

> **"We have the ability to change rules and implement rules in real time. So I could write Rule 1, 2, 3, 4, look at it in the sandbox, see how it would affect real data, and if it doesn't crush false positives or increase number of cases coming through, we implement it."**
>
> *SVP of digital payments, financial services*

- **Decreased transaction friction and in-tact customer experience due to faster risk scoring (in milliseconds).** The rise of real-time payments required customers to increase the speed of risk scoring — or risk creating a poor experience. The chief security officer shared: "Before, we might have had an hour a day to conduct risk scoring to have confidence that it was an authentic, legitimate transaction. Now it has to be evaluated at the speed of light; we're talking 0.2 of a second. This introduced a significant challenge. We need a powerful tool like IBM Safer Payments that can perform that task." Today, a transaction decline or slow processing can have financial consequences for organizations because customers will use a different payment method or stop transacting with that organization.

- **Improved employee experience.** Arming analysts with IBM Safer Payments improved their work experience and happiness. The director of fraud shared: “My analytics team loves working in the IBM Safer Payments system. The flexibility that they have, the creativity that they can express around rule-writing, it’s definitely their preferred tool versus our legacy system.” Providing the proper technologies and tools that empower employees to do their jobs better increases engagement and job satisfaction, decreases turnover, and improves company culture.

“With IBM Safer Payments, we are protecting our reputation and brand. We are optimizing an environment for our staff where now they feel they’re equipped to face this challenging and dynamic environment. So it’s been good for culture, talent acquisition, retention, and morale.”

Chief security officer, banking

- **Extended solution effectiveness due to evolution with an open environment, resulting in a longer-term investment.** One challenge financial institutions face is the decreasing effectiveness of fraud management tools. The chief security officer shared: “With the advancement of technology and with the bad guys having the latest technology, there’s always an imbalance and challenge in fraud management. The tools don’t necessarily become redundant quickly, but their effectiveness curve will flatline.” With IBM’s open platform design, the solution constantly evolves, increasing the lifetime of the tool.
- **Deeper relationships with clients by collaborating and offering controlled access to rule sets.** Customers increased the level of interaction with their clients, deepening relationships. The director of fraud noted: “Unlike our previous solution, we now have the ability to open the system to our clients to work cases or manage their own rule sets. It has been a relationship-builder because now we’re in a partnership and we’re collaborating. It is a positive direction for our client relationships.”

FLEXIBILITY

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

- **Host IBM Safer Payments in the cloud.** IBM Safer Payments is an infrastructure-agnostic solution, providing customers with the same experience regardless of where the solution is deployed. This gives customers the flexibility to run on-premises, in the cloud, or a mix of both.
- **Incorporate new payment channels and data sources without great additional investment.** IBM Safer Payments is an any-and-all cashless payment channel solution, and as new channels develop, customers can incorporate these and react to the challenge of preventing fraud within them. Without IBM Safer Payments, customers would be hard-pressed to react quickly enough to new payment channels.
- **Repurpose existing resources to more value-added tasks.** Customers found that by reducing some of the workflow related to reviewing false positives (Benefit B), they were able to utilize the newfound capacity to train analysts on new skills and turn them toward more value-added tasks. The SVP of digital payments noted: “Our goal was to be able to reallocate headcount to doing more analysis verses reacting. We’ve been able to take some of our analysts that just did fraud and move them into a data scientist role. I’ve been able to trim down some of the job openings that we had available.”

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Dtr	Implementation	$275,991	$88,164	$0	$0	$364,154	$356,140
Etr	IBM licensing, support, and implementation consulting	$690,000	$1,817,000	$1,909,000	$2,001,000	$6,417,000	$5,422,885
Ftr	Ongoing management	$0	$390,500	$484,000	$577,500	$1,452,000	$1,188,884
	Total costs (risk-adjusted)	$965,991	$2,295,664	$2,393,000	$2,578,500	$8,233,154	$6,967,909

IMPLEMENTATION

Customers incurred both indirect labor costs and direct costs for purchasing additional hardware. Experiences of the interviewed organizations include:

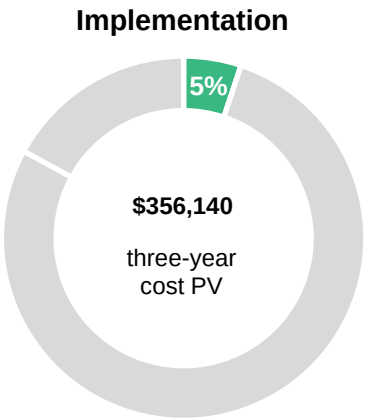
- **Business and technical resources for implementation.** The SVP of digital payments described the composition of the implementation team: “On our side, we had fraud team representation and people from the payments development team. We also had an architect and several developers. There was a business analyst, a product owner, someone who led our development team, and management representation. Overall, it was a typical project for us. No different than any other implementation project really.”
- **A phased approach for deployment.** The chief security officer shared: “We decided that we would take a three-phased approach in terms of what channels products to focus on and in what sequence. We were biting off little bite-sized pieces, so for each phase we implemented, stabilized, tested, and then moved on to the next category. This made the implementation manageable and reduced risk.”
- **Variation duration of project (between seven months and two years).** The length of and effort required to implement IBM Safer Payments varied by organization. Customers cited implementation periods of seven months to two years, depending on the products, channels, hosting environment, and prioritization of project against other strategic endeavors. The chief security officer with the longest implementation noted: “Often these types of projects aren’t isolated. We have hundreds of projects playing out at any one time, so we needed to make sure to manage the capacity and capability required. We couldn’t implement all of IBM Safer Payments at once because it would have put a strain on other projects.”
- **Varying purchases of additional hardware to support the investment.** Hardware purchases varied from $0 to $500,000, with most organizations incurring less than $50,000 in additional hardware support costs.

Modeling and assumptions. To capture the interviewees' implementation experiences, Forrester assumes:

- The composite organization chooses to first implement IBM Safer Payments across its card product. This initial implementation takes six months.
- The secondary implementation takes an additional two months and brings the digital payments product under management of IBM Safer Payments.
- Internal resources roll on and off the implementations in waves, dedicating up to 50% of their time when needed. The internal team comprises eight resources in both technical and business roles.
- The average burdened cost for implementation resources is $8,333.
- The composite organization incurs $50,000 of costs related to the purchases of supporting hardware and servers.

Risks. These results may not be representative of all experiences; the cost will vary between organizations depending on system requirements, necessary integrations, security requirements, skill sets of existing resources, and the ability to dedicate internal resources to the implementation. Other factors to consider include:

- Customers may choose to host IBM Safer Payments in a public cloud, in which case there would be additional hosting costs.
- Customers may also incur additional costs for training outside of the implementation period.
- Only one interviewed organization had significant time dedicated to training: three days of super user training and up to 6 hours of training for analysts.



- Customers may have several more products (e.g., digital payments, credit card payments, debit card payments), and the integration of these channels may increase the duration of implementation and therefore increase internal costs.

To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $356K.

Implementation						
Ref.	**Metric**	**Calculation**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Number of implementation months	Interviews	6	2		
D2	Internal FTEs dedicated to implementation	Interviews: 8 FTEs at 50% dedication	4	4		
D3	Monthly burdened cost of resources (rounded)	$100,000/ 2 months	$8,333	$8,333		
D4	Subtotal: Internal labor costs	D1*D2*D3	$199,992	$66,664		
D5	Supporting hardware and server costs	Interviews	$40,000	$10,000		
Dt	Implementation	D4+D5	$239,992	$76,664	$0	$0
	Risk adjustment	↑15%				
Dtr	Implementation (risk-adjusted)		$275,991	$88,164	$0	$0
	Three-year total: $364,154			**Three-year present value: $356,140**		

IBM LICENSING, SUPPORT, AND IMPLEMENTATION CONSULTING

IBM Safer Payments is offered as a Term License (monthly), Committed Term License (CTL), or Perpetual License. Payment is typically made either upfront or financed by IBM Global Finance (IGF), which is subject to evaluation. The interviewees purchased Perpetual Licenses or CTLs to own the IBM Safer Payments software, which includes a certain number of transactions. The best way to determine licensing costs is to speak directly with an IBM representative.

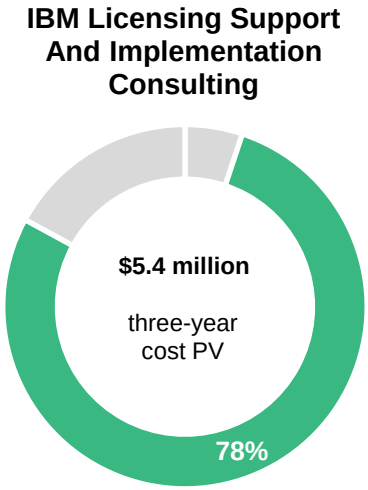
Customers also incurred costs related to the consulting services from IBM during the implementation of IBM Safer Payments. IBM Lab Services or one of IBM's Certified Business Partners can provide implementation services; these may have different pricing points. When provided by Lab Services, the implementation includes know-how transfer/training so that clients may become independent on their use-case expansion.

Modeling and assumptions. To capture the interviewees' experiences, Forrester assumes:

- The composite organization signs a CTL with IBM, which includes subscription and support. The CTL covers approximately 800 million transactions per year. The composite finances the license through IGF, and therefore the licensing costs have been allocated across the three-year period under analysis.
- IBM supports the implementation for a one-time fee of $600K, which covers the implementation of two use cases: the card and digital channels.

Risks. These results may not be representative of all experiences; the cost will vary between organizations depending on volume of transactions, discount levels, length of contract, and existing relationship with IBM.

To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $5.4 million.



IBM Licensing, Support, And Implementation Consulting

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	Three-year committed term license agreement and support costs	Composite		$1,580,000	$1,660,000	$1,740,000
E2	IBM implementation consulting	Composite	$600,000			
Et	IBM licensing, support, and implementation consulting	E1+E2	$600,000	$1,580,000	$1,660,000	$1,740,000
	Risk adjustment	↑15%				
Etr	IBM licensing, support, and implementation consulting (risk-adjusted)		$690,000	$1,817,000	$1,909,000	$2,001,000
	Three-year total: $6,417,000			**Three-year present value: $5,422,885**		

ONGOING MANAGEMENT

IBM Safer Payments works best with ongoing management and improvements. The director of fraud prevention, who had the most extensive ongoing management use case, explained: “We have several different people that do ongoing management of the solution. We have the operations team manager, who does case management configuration. Then we have a couple of guys that are not 100% dealing with IBM Safer Payments, but they manage and change the rules, run simulations. And then finally, we have a small team of two and a half data scientists.” Other customers had smaller ongoing management teams and fewer data scientists.

For some of the interviewed organizations, ongoing tuning and optimization of the solution required no additional headcount, but the SVP of digital payments shared: “There was some expectation that headcount would be reduced as an outcome of the IBM Safer Payments investment. I actually made the opposite argument because IBM Safer Payments provides a much more comprehensive scanning of activity.” IBM empowered the interviewed organizations to do more with the same number of resources, and it also empowered analysts to take more control of rule-building and provided opportunity to create a more sophisticated approach to fraud management.

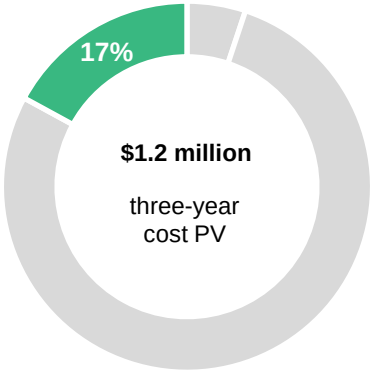
Modeling and assumptions. To capture the interviewees’ experiences, Forrester assumes:

- The composite has one dedicated operations manager assigned to managing IBM Safer Payments.
- The operations manager has a burdened annual cost of $100,000.
- The composite reallocates or hires between three and five analysts to improve its fraud management practices. These analysts are a mix of on- and offshore resources.
- The burdened annual cost of an analyst is $85,000.

Risks. These results may not be representative of all experiences; the cost will vary between organizations depending on existing skill sets and capacity, burdened cost of on- vs. offshore resources, and IBM Safer Payments use cases. Operations mangers are likely already in place, and therefore there would be no additional cost to include this ongoing management role. Additionally, customers may be able to maintain existing analyst headcount when transitioning to IBM Safer Payments. Readers should evaluate existing capacity and plan accordingly.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $1.2 million.

Ongoing Management



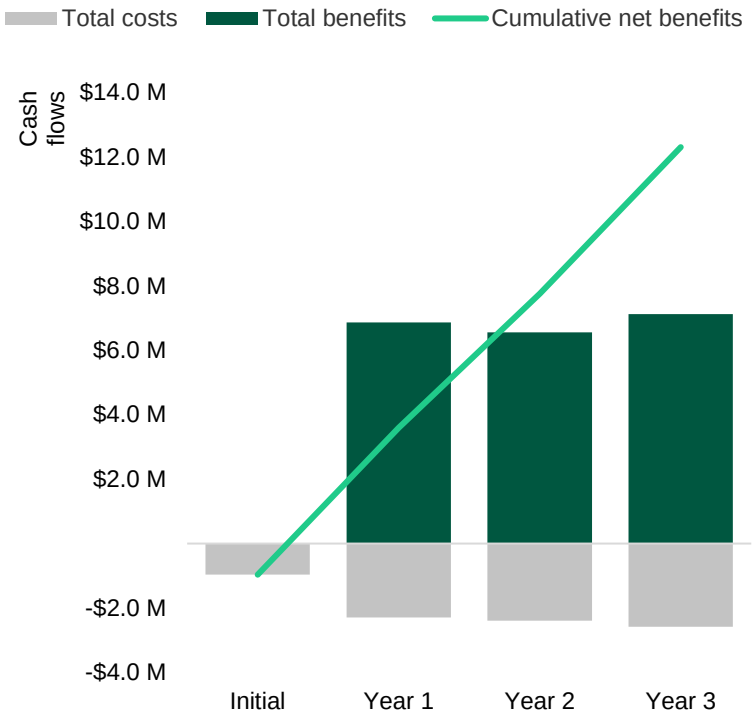
Ongoing Management

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	Number of operations managers dedicated to IBM Safer Payments	Composite		1	1	1
F2	Operations manager annual burdened cost	Composite		$100,000	$100,000	$100,000
F3	Number of additional analysts	Interviews		3	4	5
F4	Burdened cost of analysts	Composite		$85,000	$85,000	$85,000
Ft	Ongoing management	(F1*F2) + (F3*F4)	$0	$355,000	$440,000	$525,000
	Risk adjustment	↑10%				
Ftr	Ongoing management (risk-adjusted)		$0	$390,500	$484,000	$577,500
	Three-year total: $1,452,000			**Three-year present value: $1,188,884**		

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	($965,991)	($2,295,664)	($2,393,000)	($2,578,500)	($8,233,154)	($6,967,909)
Total benefits	$0	$6,860,220	$6,554,404	$7,122,730	$20,537,354	$17,004,839
Net benefits	($965,991)	$4,564,556	$4,161,404	$4,544,230	$12,304,200	$10,036,930
ROI						144%
Payback period (months)						<6 months

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."

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.


FORRESTER®