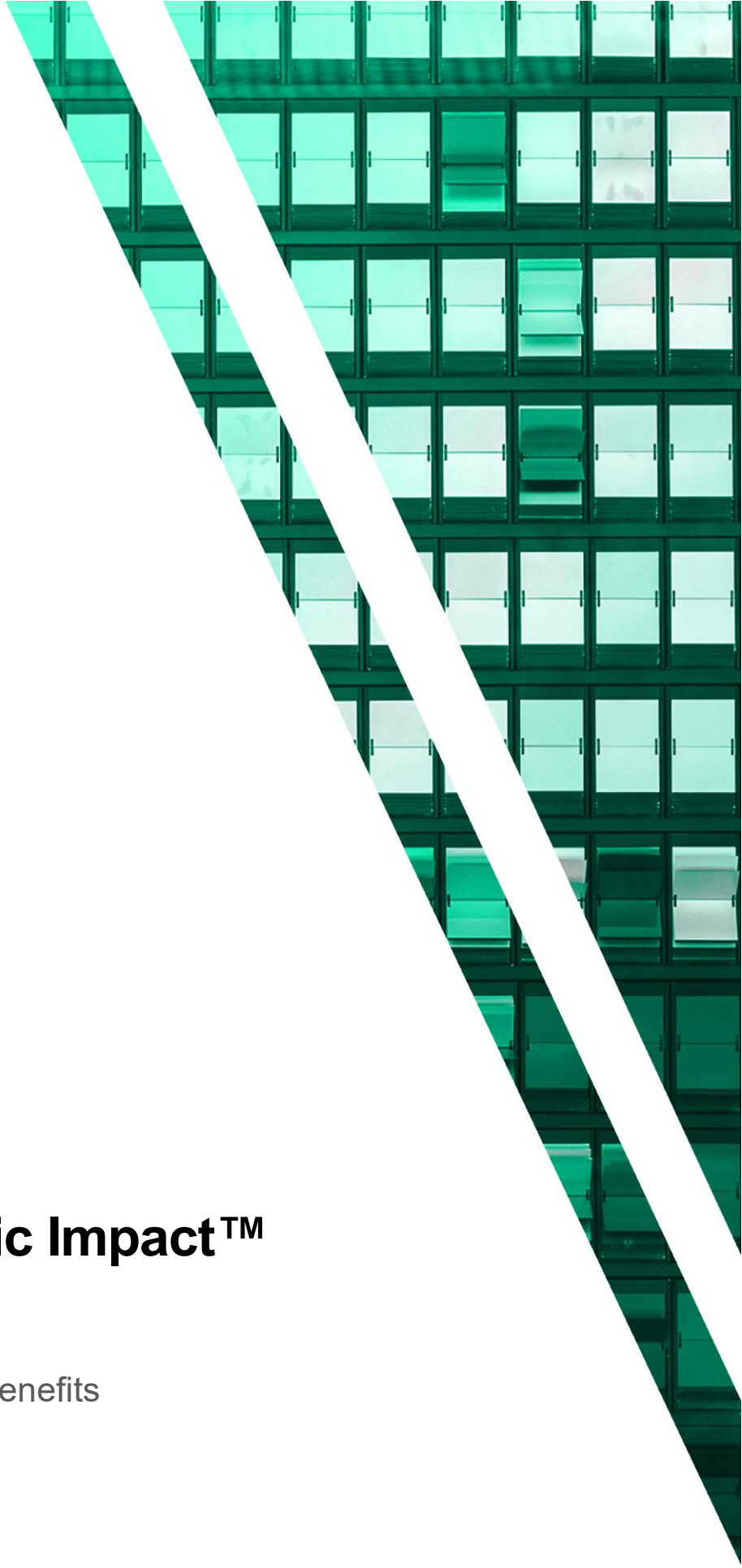
FORRESTER®



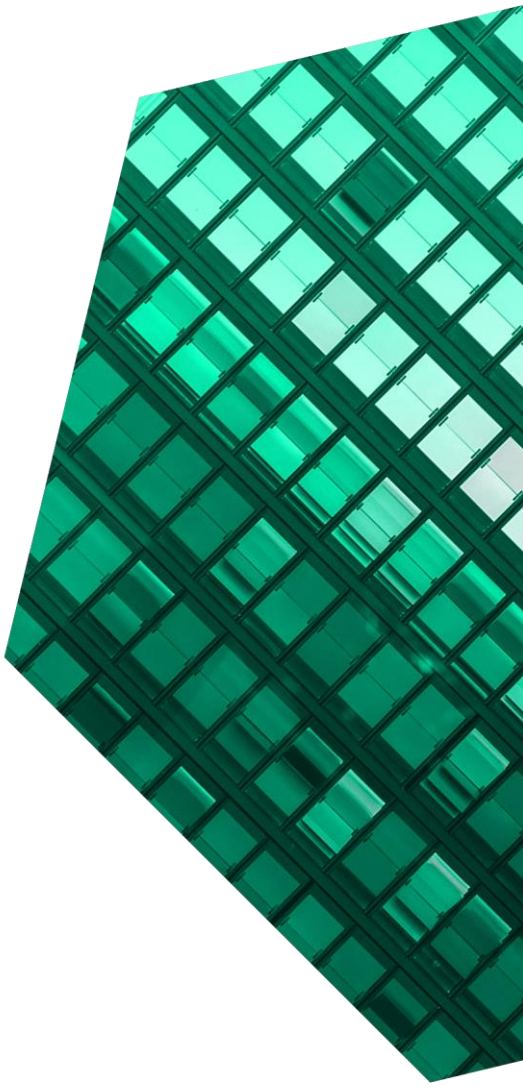
The Total Economic Impact™ Of Sardine

Cost Savings And Business Benefits Enabled By Sardine

DECEMBER 2023

Table Of Contents

Consulting Team: Henry Huang
Chengcheng Dong
Marianne Friis



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

Organizations with online businesses use digital fraud management solutions to reduce financial fraud, reduce fraud investigation costs, and bolster the customer experience.[1] Digital fraud management is built into every interaction with customers, including enrollment, authentication, and transactions. Besides conventional data from credit files, physical identity documents, phone numbers, and email addresses, new sources of data like device fingerprint analytics and behavioral biometrics can help reduce identity theft.

Sardine's platform provides both behavioral signal data and device-level data to capture suspicious activities and help online businesses prevent fraud and process payments.

Organizations with online businesses traditionally invested in identity verification (IDV) to primarily reduce identity theft. Due to the challenging environment, these organizations needed to deploy multilayered digital fraud management (DFM) solutions to collect data and detect identity fraud — like account takeover (ATO) or opening of fraudulent accounts — as well as payment fraud, like stolen cards payments and automated clearing house (ACH) kiting. The new source of data includes device fingerprint analytics and behavioral biometrics. With this comprehensive DFM, organizations can reduce financial fraud and decrease chargebacks.

On the other hand, organizations rely on DFM vendors to reduce fraud investigation costs. The qualified DFM solutions should be able to improve investigators' productivity and effectiveness when the internal investigation teams are doing manual reviews. What's more, organizations expect DFM vendors to make accurate decisions (i.e., provide both a low false positive and a low false negative rate) to reduce the rejections of legitimate customers and legitimate transactions. This means lower customer attrition, higher retention, and an improved overall customer experience.[2]

KEY STATISTICS

Return on investment (ROI)
230%

Net present value (NPV)
$6.84M

Sardine commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Sardine.[3] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Sardine on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives with experience using Sardine.

Fraud reduction rate due to automation

9%

For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a B2C financial services organization that implements Sardine in the customer onboarding process and transactional level to prevent fraud.

Prior to using Sardine, these interviewees noted how their organizations faced an increasing fraud rate. By using traditional DFM vendors or in-house rule-based solutions, the organizations decided with incomplete information to avoid new fraudulent accounts and transactional fraud. What's more, organizations were experiencing more first-party or friendly fraud that abused policies. All those challenges resulted in rising chargebacks and financial loss as well as fraud investigation costs. Organizations realized that they needed to implement advanced DFM solutions with business policy definition rules and access to consortium data.

After the investment in Sardine, the interviewees' organizations obtained end-to-end DFM workflows to prevent fraud. Organizations gained intelligence to prevent know-your-customer (KYC) and know-your-business (KYB) fraud in customer acquisition and gained device intelligence and behavioral biometrics to stop fraudulent accounts at the point of account opening and transactional fraud. More importantly, organizations saw a reduction in false positives of new sign-ups while filtering out fraudulent new account openings. Key results from the investment include fraud mitigation, operations efficiencies, and valid pass rate improvement.

KEY FINDINGS

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

- **A 9% reduction in fraud rate.** The composite organization implements Sardine to collect behavior anomalies during the account opening process, such as copying and pasting SSNs or taking an unusually long time to type the DOB, to detect possible fraud and also monitor VPN access during the transactional process. All the data automatically collects and contributes to the approval or rejection decision, which decreases general fraud and avoids bad actor account activations for the organization. On the other hand, Sardine detects payment fraud in the transaction process stage to lower the rate of chargebacks. The overall fraud rate can be decreased by 9% with the deployment of Sardine. Over three years, fraud mitigation saves $2.29 million for the composite organization.
- **Fraud investigations completed 50% faster.** Suspicious applications or possibly fraudulent transactions at the composite organization go to fraud analysts for manual review, depending on its rules. With Sardine's deployment, the number of cases that need to be reviewed decreases. Sardine's scoring mechanism provides a strong basis for manual review, which increases review efficiency. Over three years, the savings in analysts' time and increases in efficiency equal $2.40 million for the composite organization.
- **A 11% decrease in false positives.** Sardine decreases the false positive rate by 11% for the composite organization compared to previous vendor solutions. By decreasing the false positive rate, more legitimate customers can open accounts with the composite organization and bring more value. Over three years, the composite organization realizes an $5.13 million increase in profit.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Simplicity and efficiency.** Sardine's sophisticated algorithm and rules provides a simple workflow and user-friendly interface to the composite organization. There is limited training and a short ramp-up phase required for the composite organization to implement Sardine.

- **Legacy vendor solutions consolidation.** By implementing Sardine, the composite organization can consolidate certain legacy vendor solutions depending on its previous workflow or integrate Sardine into the previous workflow to enhance fraud detection.
- **Access to consortium data.** With conventional databases or traditional data points, the composite organization can hardly detect ATO or first-party fraud. With Sardine, the composite organization can gain access to consortium data to prevent evolving fraud behaviors.
- **Proactive support from Sardine's fraud and compliance teams.** The composite organization receives proactive support from the Sardine team. The Sardine team helps the organization refine the rules based on the organization's needs, provides industry updates, and summarizes the lessons learned from the fraud it captured. All the support makes the composite organization more professional and productive in fraud prevention.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **The cost of Sardine licensing totaling $2.65 million in three years.** Sardine uses a hybrid cost model. It includes an upfront fixed fee for integration and variable costs depending on the number of transactions. Based on the size and the usage of the composite organization, the three-year cost of Sardine licensing cost is $2.65 million.
- **The internal costs related to Sardine deployment totaling $320,000.** To implement and maintain the Sardine solution, the composite organization needs to have its risk management and fraud analysts refine the data and rules constantly. Based on the size and the usage of the composite organization, the three-year internal cost is $320,000.

The representative interviews and financial analysis found that a composite organization experiences benefits of $9.81 million over three years versus costs of $2.97 million, adding up to a net present value (NPV) of $6.84 million and an ROI of 230%.

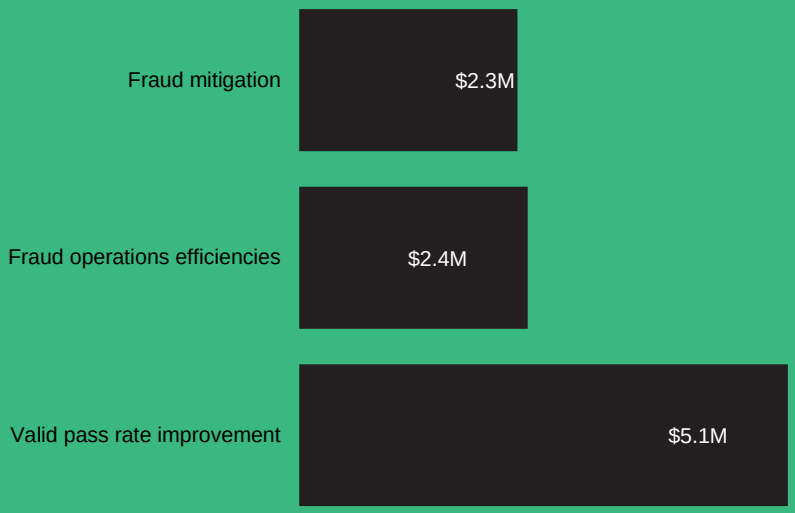
ROI
230%

BENEFITS PV
$9.81M

NPV
$6.84M

PAYBACK
<6 months

Benefits (Three-Year)



“We picked Sardine because it was the simplest thing to integrate with. We prioritize all our decision-making on what is the simplest to implement and actually iterate through things really quickly. We felt that Sardine gives us the biggest bang for the buck in terms of effort.”

— VP, financial services

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 Sardine.

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 Sardine can have on an organization.

DUE DILIGENCE

Interviewed Sardine stakeholders and Forrester analysts to gather data relative to Sardine.

INTERVIEWS

Interviewed six representatives at organizations using Sardine to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' 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 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.

The Sardine Customer Journey

Drivers leading to the Sardine investment

Interviews			
Role	**Industry**	**Region**	**Total Revenue**
Compliance and risk manager	Financial services	US and India	$5 million
Director of fraud strategy	Financial services	US	-
Chief technology officer	E-commerce	US	$300 million
Chief risk and information security officer	Financial services	US	$60 million
Vice president	Financial services	US	Several millions
Product manager	Financial services	Canada and Australia	-

KEY CHALLENGES

Four of the interviewees' organizations had different DFM vendor solutions built into their customer onboarding and transactional processes. The other two organizations used in-house build solutions to prevent fraud, mainly rule-based solutions. The interviewees noted how their organizations struggled with common challenges, including:

- **Increasing fraud rate and chargebacks.** Fighting against different types of fraud is a consistent challenge for financial services organizations and e-commerce organizations during both the customer onboarding and transactional phases. With legacy DFM vendor solutions or in-house-built solutions, organizations were experiencing a rising fraud rate since the traditional methods couldn't catch up with evolving fraud behaviors. The product manager of the Canadian and Australian financial services organization commented: "Before Sardine, we had a challenge [with] fraud. So, the fraud comes in as using a fake identity to join us and some scammers try to manipulate our senior customers to do a lot of things. Also, a lot of investment scams and romance scams are going on as well as some friendly frauds. We were getting chargebacks from our banks."
- **Siloed solutions caused data isolation**. Due to regulations, organizations in the financial services industry often had different required fraud-prevention solutions. However, the different solutions couldn't be integrated, causing silos. The chief risk and information security officer with the financial services organization in the US shared: "It was very siloed. On the bank side, the bank data was the bank data. That data [came from two sources]. On the fintech side, the data stayed in another two different sources … Then we would get oversight reports and access to the data as needed but it was never brought together into one database or platform to say what are the specific anomalies."
- **Less effective with traditional data points.** Fraudsters' behavior and technology were evolving. Traditional fraud prevention methods worked less effectively since the data they captured was not able to reflect true intentions. For example, the director of fraud strategy with

the financial services organization in the US shared that using VPN was a fraud signal before with legacy vendor tools but it was not an effective metric for fraud detection. They shared: "A lot of the traditional data points that we were leveraging were not as effective as they used to be because of swooping technology and just the sophistication in the attack vectors. A huge majority of the population uses a VPN. So, it's no longer an indication that it's fraudulent or sketchy. We were looking at newer, innovative approaches to fighting fraud, and we had the opinion that behavioral-based fraud fighting is going to be a key trend in the future because it's much harder to spoof and it takes far more time to spoof behavioral stuff."

- **Legacy solutions with costly maintenance.** Organizations spent a fortune to use solutions built internally or vendor solutions to prevent fraud. With increased business demand, the cost was too high to bear. The CTO with the e-commerce organization said: "We had invested a lot of money into developing our own risk solution. Over time, we found it was very costly to maintain. We experienced all sorts of chargebacks and sizable events."

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Effectively reduce the fraud and chargeback rates.
- Use advanced technology to collect data and evolve with fraudsters' behavior.
- Have a unified dashboard and one system throughout the organization to eliminate siloed solutions and promote collaboration.
- Be cost-effective.
- Be integrated with existing technology stacks.

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 six interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The midsize global B2C financial services and insurance institution provides conventional financial services. The composite organization has a strong brand, a large customer base, and a strong online and offline presence.

Deployment characteristics. The composite organization is a global operation with a focus in the US. Previously, it used a rule-based fraud prevention solution with integrated vendor solutions mainly using public information for verification. The composite organization deploys Sardine in its customer onboarding and payment stage to prevent transactional fraud.

Key Assumptions

- **Midsize global B2C financial services and insurance institution**
- **43,544 monthly new sign-up applications**
- **Previously used rule-based fraud detection and public information**

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 mitigation	$919,784	$919,784	$919,784	$2,759,351	$2,287,365
Btr	Fraud operations efficiencies	$963,900	$963,900	$963,900	$2,891,700	$2,397,077
Ctr	Valid pass rate improvement	$2,060,925	$2,060,925	$2,060,925	$6,182,774	$5,125,214
	Total benefits (risk-adjusted)	$3,944,608	$3,944,608	$3,944,608	$11,833,824	$9,809,656

FRAUD MITIGATION

Evidence and data. Financial services organizations face different types of fraud when interacting with customers online, from onboarding to ACH transfer to payment transactions. Sardine was typically deployed together at the interviewees' organizations with other solutions to provide comprehensive data and a holistic view of operations.

- The director of fraud strategy with the financial services organization in the US shared: "There's no one vendor out there that can outperform a suite of intelligence tools. So, [there's] always a better approach to doing something called the hybrid option, and the hybrid option is where you leverage a combination of internal modeling, rule engines, and vendors to help give a holistic view."
- Data is the key to fighting fraud, and conventional data collection can help to prevent traditional fraud behaviors. But these traditional methods can't help organizations fight fraud from advanced technology and behaviors. The director of fraud strategy with the financial services organization in the US said: "We were looking at newer, innovative approaches to fighting fraud. We had the opinion that behavioral-based fraud fighting is going to be a key trend in the future because it's much harder to spoof — it takes far more time to spoof behavioral stuff. So, when Sardine came out with its behavioral biometric product, we know that, okay, the behavioral biometrics component is probably the game changer."
- During the onboarding process, Sardine detected fraud at interviewees' organizations by collecting data on customer behaviors when inputting data as well as device information. The product manager with the financial services organization in Canada and Australia shared: "Our understanding is that Sardine is very good at device intelligence and behavioral biometrics. Our operations team relies on Sardine's dashboard to give us additional insights regarding [a user's] device, their phone numbers, email, and the last location, which helps us make a better call with respect to risk."

  Interviewee's organizations experienced a significant impact on customer onboarding rate. The director of fraud strategy with the financial services organization in the US reported: "For onboarding, it [flagged] about 3% of our applications, 3% of applications that were not caught by the other traditional vendors. Three

percent is highly valuable because it's all based on behavior."

- Sardine also had a huge impact on chargebacks. The product manager with the financial services organization in Canada and Australia reported that the organization faced 10 to 15 chargeback cases of fraud every month. After the implementation of Sardine, the number of chargeback cases dropped to two to three per month.
- Financial organizations also implemented Sardine to prevent ACH fraud. The director of fraud strategy with the financial services organization in the US shared: "ACH fraud is a different beast, so a lot of it comes to account takeover, and then [fraudsters] are pushing or pulling funds in and out of the account, stealing them. That's a particular problem. That's why we're building up the data consortium model with Sardine on the ACH fraud side. Like, maybe 10% [of fraud] falls under that synthetic identity side."

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following about the composite organization:

- The composite organization receives 522,526 new account applications each year.
- With Sardine deployment, the total fraud reduction rate (including IDV fraud and payment fraud) is 9%. For general fraud cases, the likelihood of it happening is 1%.
- Based on Forrester data, each general fraud case costs the composite organization $2,301.

Risks. Risks that could impact the realization of this benefit include:

- An organization's previous verification rules and pass rate, as well as the rules on transactional-level fraud prevention.
- The data sources of the previous verification vendors.
- The average transaction value, as well as the transaction alert threshold.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.29 million.

Fraud Mitigation

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	New customer accounts	Interviews	522,526	522,526	522,526
A2	Fraud reduction rate on account applications, automation based	Interviews	9%	9%	9%
A3	Cost per general fraud	Forrester internal research	$2,301	$2,301	$2,301
A4	Likelihood of general fraud	Forrester internal research	1.0%	1.0%	1.0%
At	Fraud mitigation	A1*A2*A3*A4	$1,082,098	$1,082,098	$1,082,098
	Risk adjustment	↓15%			
Atr	Fraud mitigation (risk-adjusted)		$919,784	$919,784	$919,784
	Three-year total: $2,759,351			**Three-year present value: $2,287,365**	

FRAUD OPERATIONS EFFICIENCIES

Evidence and data. Sardine's automation eliminated manual work in the fraud prevention process of interviewees' organizations. By deploying Sardine, the organizations experienced increased efficiency among the fraud team members.

- With the elimination of manual work, the fraud prevention team can reallocate their time to other strategic tasks or their position can be reallocated to other high-level positions. The CTO with the e-commerce organization said: "It's the effectiveness of what the teams are doing. We're able to spend more time on other customer-focused operations rather than some of the risk operations … With the increased visibility we have increased operational efficiencies."
- Sardine had a robust dashboard to present the data and help teams at the interviewees' organizations with reporting. The chief risk and information security officer with the financial services organization in the US said: "There is a reporting element inside the Sardine dashboard that aggregates data and brings it together. As part of our monthly oversight processes, I would say we're probably saving about 25% [of the time we spent before]."
- With a decreased fraud rate after the implementation of Sardine, the fraud teams saved lots of effort on post-fraud tasks. The product manager with the financial services organization in Canada and Australia spoke highly about Sardine's ability to help the team: "Previously, 70% of fraud analysts' time went to fraud. Now, I would say around 30% of their time now goes to fraud. There is a 40% reduction in their effort to fight fraud. Previously, when we detected fraud, we have to first investigate. Then we have to create those STRs [suspicious transaction reports]. Those reports go to different regulators, and they have to download and prepare those reports. There is a long process of doing this stuff, but if we prevented it earlier, then … we don't have to do those things."

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following about the composite organization:

- The composite organization sees a 50% reduction in the time spent by the fraud analysts on their previous workloads.
- The composite organization maintains a fraud team of 16 full-time specialists with fully loaded compensation of $141,750 per year, or $68 per hour.

Risks. Risks that could impact the realization of this benefit include:

- Fraud team headcount.
- Time spent by fraud specialists on fraud prevention and setting rules, as well as post-fraud tasks.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $2.40 million.

Fraud Operations Efficiencies					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Reduction in fraud analyst time spent	Interviews	50%	50%	50%
B2	Number of fraud specialists	Interviews	16	16	16
B3	Fraud specialist annually fully loaded salary	Forrester standard	$141,750	$141,750	$141,750
Bt	Fraud operations efficiencies	B1*B2*B3	$1,134,000	$1,134,000	$1,134,000
	Risk adjustment	↓15%			
Btr	Fraud operations efficiencies (risk-adjusted)		$963,900	$963,900	$963,900
	Three-year total: $2,891,700			**Three-year present value: $2,397,077**	

VALID PASS RATE IMPROVEMENT

Evidence and data. Interviewees constantly reported a decreased false positive rate of alerts after the implementation of Sardine. This led to an increase in onboarding legitimate customers who brought profit to interviewees' organizations.

- The director of fraud strategy said their financial services organization in the US experienced a 5% decrease in false positives. They described how Sardine helped the onboarding process by using biometrics data: "We use Sardine for behavioral biometrics during onboarding and to give us intelligence about how the customer is acting on their journey in particular. Are they copying and pasting their social security numbers into the field? Are they spending more than five seconds typing out their last name? Are they using multiple screens and moving the mouse across different screens while filling out the field? These are all obviously very high-risk indicators that it's not memory based, which is what you want to look for."
- The chief risk and information security officer with the financial services organization in the US reported: "I do believe that false positives are definitely down because of the way [Sardine] attacks the synthetic fraud component. I think it's only going to get better over time. I think it's going to be around at 15% to 20% range on true synthetic fraud."
- The Sardine team worked with interviewees' organizations on a case-by-case basis to reduce their false positive rate and remove the friction in the onboarding process. The product manager with the financial services organization shared how Sardine worked with the organization to set the rules: "For the rules with high false positive [rates], we were able to go back to Sardine and ask them to tighten the screws or add [details]. In the end, it resulted in a system where [we had] very high true positive rules set up to automatically decline. The rules that had a decent true positive rate but were not devoid of false positives were routed for manual review. And we also calibrated [them] in such a way that it was the registration of alerts for us that our operation team can handle. Overall, we realized the false positives were declining."
- Besides the fall of false positive rates, Sardine also brought up the organizations' true negative rates, which helped them reject fraudsters in the

onboarding process. The director of fraud strategy with the financial services organization in the US shared: “I would say about 3% of our applications are flagged as unapproved by Sardine. Three percent of applications were not caught by the other traditional vendors. This 3% is highly valuable because it’s all based on behavior.”

Modeling and assumptions. To calculate the value of this benefit, Forrester assumes the following about the composite organization:

- With the deployment of Sardine, the composite organization experiences an 11% increase in the pass-through rate due to an effectively reduced false positive rate.
- The average three-year value of a customer is $224 for the composite organization[4].
- On average, the composite organization has 104,505 new potential customers who bring value.

Risks. Risks that could impact the realization of this benefit include:

- The organization’s previous verification pass rate.
- The number or percentage of onboarded customers that contribute to revenue.
- The business value per customer.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $5.13 million

Valid Pass Rate Improvement

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Pass-through rate percentage point increase	Interviews	11%	11%	11%
C2	New potential customers per year	Composite	104,505	104,505	104,505
C3	Total newly onboarded customers attributable to Sardine	C1*C2	11496	11496	11496
C4	Average three-year value of a multichannel financial institution customer	Forrester research	$224	$224	$224
Ct	Valid pass rate improvement	C1*C2*C4	$2,576,156	$2,576,156	$2,576,156
	Risk adjustment	↓20%			
Ctr	Valid pass rate improvement (risk-adjusted)		$2,060,925	$2,060,925	$2,060,925
	Three-year total: $6,182,774			**Three-year present value: $5,125,214**	

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Sardine offered simplicity and efficiency to prevent complex fraud behaviors.** Multiple interviewees mentioned that Sardine provided a simple workflow and user-friendly interface to their organization. The organizations didn't need to have a team of fraud experts to work with Sardines to set up fraud prevention rules or integrate it with the existing workflow. The VP with the financial services organization said: "I think the most important thing for us is simplicity and efficiency. As a startup, it's meeting our targets and it's taking care of everything for us so we don't have to worry about it and we can just focus on building our product."
- **With Sardine's deployment, organizations experienced different levels of savings from consolidating legacy vendor solutions.** Sardine includes over 35 data vendors integrated in its platform. The interviewees' organizations have no need to use different vendors in order to access different databases. Different organizations experienced different levels of savings on legacy vendor solutions depending on the previous technology stack. The director of fraud strategy with the financial services organization in the US reported that their organization replaced some fraud prevention vendor solutions with Sardine and said, "The amount of money that we saved from turning off vendors paid probably the Sardine cost [two times over]." The VP with the financial services organization shared that their organization used a waterfall approach and deployed Sardine to prescreen its customers. The VP stated: "We used Sardine before KYC and now our KYC rate is significantly higher because Sardine catches people and Sardine is much cheaper than KYC. Sardine is catching a lot of the bad actors and actually saving us money downstream on the KYC."
- **Sardine offered access to consortium data and organizations benefited from it.** The amount and quantity of data is one of the key factors to preventing fraud. By deploying Sardines, interviewees' organizations were able to access consortium data that they can't gain access before. The CTO with the e-commerce organization said: "Sardine has consortium data. If there's a known card in the system that's identified as fraudulent or a phone that's identified as fraudulent, not even through our transaction, but through [an organization with] the consortium data, then we're able to benefit from that." The director of fraud strategy with the financial services organization in the US shared that with access to consortium data, the organization was able to identify the ACH fraud, which was 10% of their fraud cases.
- **Sardine team provided proactive support to the organizations.** Interviewees viewed the Sardine support team as their partner because of the proactive support Sardine provided. The product manager with the financial services organization in Canada and Australia said: "Sardine is one of the positives that I see is they have a very good support team. We have a biweekly call set up with them. The team provided us with a very good guide, and they also brought in an expert within their team." The VP with the financial services organization said: "I view them as our fraud team for all intents and purposes. But the difference is that if there was a fraud team, there would be daily communication with the fraud team and all of that; here it's more like an outsourced fraud team I would say."

FLEXIBILITY

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

- **Helping the expansion of business to new financial services segments.** One interviewee noted that having Sardine in their process was beneficial if they were entering new business segments, like cryptocurrency trading, NFT, or neo bank, since traditional vendors can't collect the data that is suitable for the new business. The CTO with the e-commerce organization said: "We want to enable being able to purchase our product with crypto in the future, that's kind of a natural extension of the business that Sardine is in. They kind of focus on the high-risk crypto industry anyway, and they were able to extend this out to our model as well. I think the way they've approached the design of the system is very scalable and relevant to what we were looking to do."
- **Enabling the quick deployment of new technology.** One interviewee thought Sardine enabled the organization to jump ahead on new technology and be proactive. The chief risk and information security officer with the financial services organization in the US said: "We were trying to be proactive with our build-out and jump ahead here. We try to stay a step ahead of fraud, cybersecurity, and things like that. So, when opportunities come up, we don't have a six to 12-month build-out. We have something in place that can handle the situation at hand."

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	Cost of Sardine licensing	$5,250	$1,067,297	$1,061,810	$1,061,810	$3,196,167	$2,650,803
Etr	Internal costs related to Sardine	$224,565	$38,313	$38,313	$38,313	$339,504	$319,844
	Total costs (risk-adjusted)	$229,815	$1,105,610	$1,100,123	$1,100,123	$3,535,671	$2,970,647

COST OF SARDINE LICENSING

Evidence and data. The pricing model of Sardine includes fixed and variable costs. The fixed cost depends on the size and industry of customer organizations, and the variable cost depends on the services deployed and usage.

- As of this study, there are three parts of the fixed cost of deploying Sardine. The fraud and compliance dashboard fee covers dashboard analytics, account management, and fraud analysis. The services and support fee cover the premium support provided by the Sardine team. The integration fee covers the services provided during the implementation phase.
- The majority financial services organizations of the interviewees deployed Sardine services like device and behavior, onboarding, and payment fraud. All their service fees were tired according to the usage and transactions processed through API.

Modeling and assumptions. To calculate the cost, Forrester assumes the following about the composite organization:

- The composite pays $5,000 in integration fees during the implementation phase.
- Other annual fixed costs cover the fraud and compliance dashboard fee, as well as premium support provided by Sardine team. This equals $90,000 per year.
- On the variable cost side, the composite organization chooses to deploy device intelligence and behavioral biometrics services, onboarding services, and payment fraud prevention services. This starts out at $926,473 in Year One and then settles at $921,248 in Year 2 and Year 3.
- Pricing may vary. Contact Sardine for additional details.

Risks. This cost can vary across organizations due to:

- Previous fraud technology environment.
- Number of new applications, transactions processed.
- Size and geography of the organization.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.65 million.

Cost Of Sardine Licensing						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Sardine integration fee	Composite	$5,000			
D2	Sardine fixed cost	Composite		$90,000	$90,000	$90,000
D3	Sardine usage fee	Composite		$926,473	$921,248	$921,248
Dt	Cost of Sardine licensing	D1+D2+D3	$5,000	$1,016,473	$1,011,248	$1,011,248
	Risk adjustment	↑5%				
Dtr	Cost of Sardine licensing (risk-adjusted)		$5,250	$1,067,297	$1,061,810	$1,061,810
	Three-year total: $3,196,167			**Three-year present value: $2,650,803**		

INTERNAL COSTS RELATED TO SARDINE

Evidence and data. DFM solutions need to be constantly adjusted and monitored to prevent evolving fraud. The rules and the data need to be refined to stay updated. Interviewees shared that Sardine was generally easier to work with in turns of initial deployment and daily maintenance.

- The director of fraud strategy commented that the implementation of Sardine was really easy for their financial services organization in the US. The organization took an A/B testing approach to capture data and refine rules. The interviewee said: “It’s really easy. We ran the rule engine. We looked at performance like which one caught more fraud, which one had a higher false positive decline rate, etc. Sardine outperformed our internal rule engine, so that’s the route we went.”
- In turns of configuration, Sardine provided a much easier way to help the interviewees’ organizations set it up. The chief risk and information security officer at the financial services organization in the US said: “Sardine does a great job giving you kind of a default configuration. Some other systems you could spend six months to a year just building rules. Sardine gives you a bunch of profiles based on what you’re trying to do and then rules that go along with it and gives you the ability to tweak it. But that allows you to really jump in and start running data through the sandboxes and understanding what results we are seeing and how those results might affect what we’re comfortable with.”

Modeling and assumptions. To calculate the cost, Forrester assumes the following about the composite organization:

- The initial integration planning and effort takes $30,000 to complete, including the costs of internal planning and system deployment.
- The composite organization needs a team of six fraud analysts on initial refinement to deploy Sardine. They use 25% of their time in the first year. To maintain the system, it takes two analysts and 15% of their efforts on a daily basis.
- The annual fully loaded compensation of risk management and fraud analyst is $116,100.

Risks. This cost can vary across organizations due to:

- The fraud management environment.
- The implementation approach as well as the technology management style.
- The resources available for implementation and ongoing management.
- The average salary for analysts involved.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $320,000.

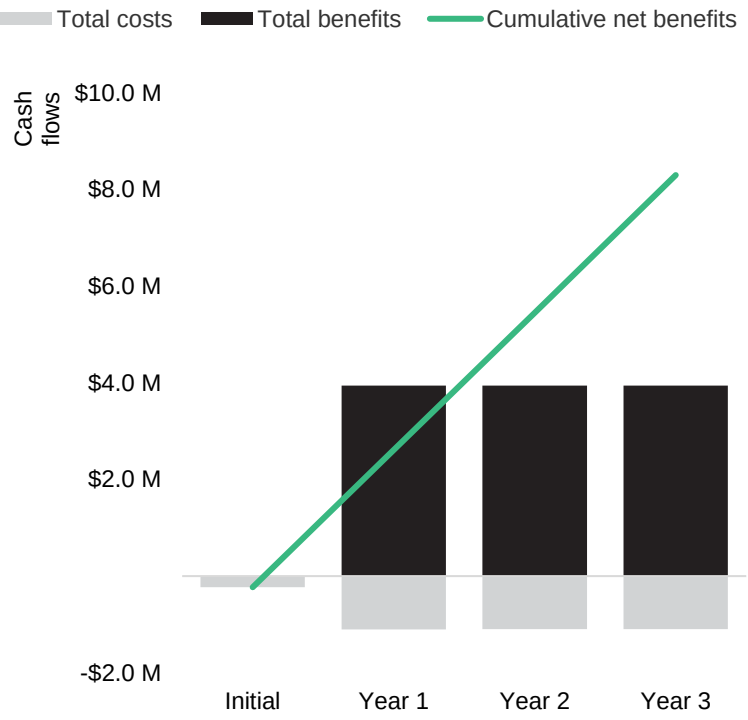
Internal Costs Related To Sardine

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Internal risk management and fraud analysts on initial refinement	Composite	6	2	2	2
E2	Percentage of time allocated data and policy refinement	Interviews	25%	15%	15%	15%
E3	Annual cost of risk management and fraud analysts	TEI standard	$116,100	$116,100	$116,100	$116,100
E4	Internal integration planning and effort	Composite	$30,000			
Et	Internal costs related to Sardine	E1*E2*E3+E4	$204,150	$34,830	$34,830	$34,830
	Risk adjustment	↑10%				
Etr	Internal costs related to Sardine (risk-adjusted)		$224,565	$38,313	$38,313	$38,313
	Three-year total: $339,504			**Three-year present value: $319,844**		

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	($229,815)	($1,105,610)	($1,100,123)	($1,100,123)	($3,535,671)	($2,970,647)
Total benefits	$0	$3,944,608	$3,944,608	$3,944,608	$11,833,824	$9,809,656
Net benefits	($229,815)	$2,838,998	$2,844,485	$2,844,485	$8,298,153	$6,839,009
ROI						230%
Payback						<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."

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

"Best Practices For E-Commerce And Retail Fraud Management In 2023," Forrester Research, Inc., February 6, 2023.

"Emerging Identity Verification (IDV) Requirements In 2023," Forrester Research, Inc., April 23, 2023.

"The Identity Verification (IDV) Landscape, Q3 2022," Forrester Research, Inc., September 6, 2022.

Appendix C: Endnotes

[1] "The Digital Fraud Management (DFM) Landscape,Q2 2023," Forrester Research, Inc., March 29, 2023.

[2] Source: Ibid.

[3] 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.

[4] "How Customer Experience Drives Business Growth, 2020," Forrester Research, Inc., December 3, 2020


FORRESTER®