The Total Economic Impact™ Of Twilio Verify

Cost Savings And Business Benefits Enabled By Verify
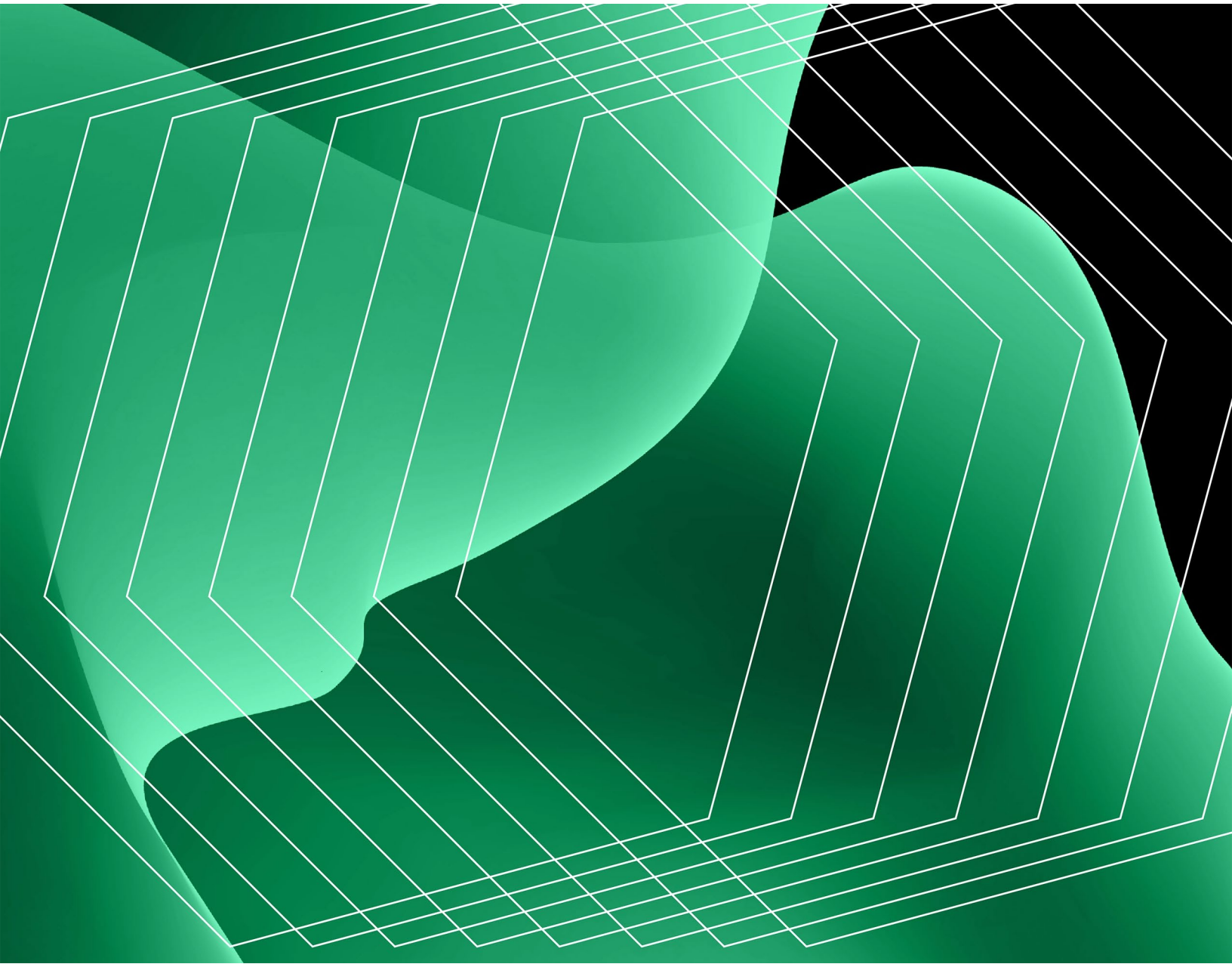
Table Of Contents

Consulting Team:

Kim Finnerty

Nikoletta Stergiou

ABOUT FORRESTER CONSULTING

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

Executive Summary

Building trust without requiring physical presence or interactions is no longer a nice-to-have but a critical requirement if businesses want to conduct secure remote transactions with minimal friction.[1] Twilio Verify addresses organizations' need for a multichannel end-user verification solution to enable two-factor authentication (2FA) in a single API. As a result, organizations could reduce costs associated with fraud, scale their operations in new markets with different requirements, and provide flexibility in their end users' experience.

Twilio Verify is a multichannel end-user verification solution that enables organizations to add two-factor authentication, including SMS one-time passwords (OTP), to their onboarding and login flow with a single API. Customers are enabled to send SMS one-time passcodes and integrate a ready-to-use solution that handles connectivity, channels, code generation, and fraud monitoring. They can also integrate any programming language with Twilio Verify's API or SDKs, and reduce fraud across multichannel with one API endpoint to validate end users and detect fraud with minimal friction. With Twilio Verify, customers can optimize two factor authentication via preferred channels like SMS with RCS upgrade, instant messaging, voice, silent network authentication, email, passkeys, push authentication, silent device approval, and Time-based One-Time Passwords (TOTP).

Twilio commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Verify.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Verify on their organizations.

Return on investment (ROI)
174%

Net present value (NPV)
$1.49M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Verify. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a $1 billion organization with an average of eight million total SMS verifications per year.

Interviewees said that prior to using Verify, their organizations were not utilizing purpose-built authentication tools. However, prior attempts yielded limited success, leaving them vulnerable to fraudulent activity and abuse like SMS pumping (i.e., artificially inflated traffic), difficulty identifying and resolving issues, and challenges in scaling globally.

After the investment in Verify, the interviewees improved conversion in their applications and were more successful in blocking SMS fraud attempts, optimizing SMS for better message delivery to customers, and expanding into new markets. Key results from the investment include accelerated market expansion, avoided loss from fraud, reduced fraud investigation and prevention efforts, and avoided delays in SMS OTP messages.

KEY FINDINGS

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

- **Accelerated market expansion worth more than $1.1 million.** Twilio Verify empowers the composite organization to meet regulatory requirements across many different markets globally. Entering new markets across a period of three years enables a 0.65% increase in the new market revenue in Year 1, 0.55% in Year 2, and 0.50% in Year 3. Over the course of three years and a 10% profit margin, this accelerated market expansion is worth more than $1.1 million to the composite organization.

- **Avoided loss from fraud of more than $900,000.** Twilio Verify offers a robust and secure authentication solution that helps organizations avoid fraud. Prior to the investment, the composite organization receives more than 1.8 million fraud alerts each year, with a 95% true positive rate of real fraud. Each alert costs the

composite organization $0.23. Over three years, the composite organization avoided more than $910,000 in loss from fraud.

- **Reduced time for fraud prevention labor by 95%.** Twilio Verify provides fraud analysts with greater visibility and understanding into the severity of fraud alerts that are filtered through. In the prior environment, 10 fraud analyst FTEs would spend 10% of their time reacting to fraud alerts. Automating and filtering more meaningful alerts with Twilio Verify reduces their time reacting to fraud alerts by 95%. Over three years, the time reduced from fraud prevention labor is worth more than $215,000 to the composite organization.

- **Avoided downtime due to route optimization by 90%.** Twilio Verify equips the organization with a reliable authentication solution that is not easily impacted by disruptions. In the prior environment, the composite experiences one significant messaging disruption per year which resulted in an average of 2 hours of downtime. Furthermore, labor efforts required to remediate and investigate the disruption require 12 software engineer FTEs and 10 hours of their time. Over the course of three years, avoided downtime due to route optimization is worth more than $92,000 to the composite organization.

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

- **End-user satisfaction.** Twilio Verify improves fraud detection and prevention and as a result further enhances their protection of end users. End users are entrusting organizations with sensitive and personal data, which can be detrimental if the proper steps are not in place with secure authentication solutions.

- **Integration with tech stack.** Twilio Verify's integration capabilities with various platforms and systems provide robust APIs that allow developers to easily integrate phone verification and authentication features into their applications. Twilio Verify also supports integration with popular programming languages, frameworks, and databases, making it easy to add verification functionality to existing systems. Additionally, it offers extensive documentation, code samples,

and developer resources to simplify the integration process and ensure a smooth implementation.

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

- **Licensing costs.** Twilio Verify offers flexible pricing options based on usage and requirements. The licensing costs for Twilio Verify depend on factors such as the number of successful verifications, the country and mobile operator of the phone numbers used, and the volume of SMS or voice messages sent. Twilio Verify follows a pay-as-you-go model, where users only pay for the specific services and resources they use.

- **Implementation costs.** Twilio Verify offers a seamless implementation experience. Steps taken in implementation include obtaining API credentials, provisioning or verifying phone numbers to be used for verification purposes, and integration with Verify into the organization's application.

- **Ongoing management costs.** Twilio Verify requires minimal ongoing management efforts related to maintaining the solution, which involves monitoring usage, performance, and security aspects of the Twilio Verify integration. Efficiencies in ongoing management are further improved by Twilio's robust monitoring and reporting tools to help organizations track and analyze the usage patterns and performance metrics.

The representative interviews and financial analysis found that a composite organization experiences benefits of $2.35 million over three years versus costs of $859,000, adding up to a net present value (NPV) of $1.49 million and an ROI of 174%.

Total value in benefits over the course of three years
$2.35 million

"We started using Twilio Verify because it had a built-in feature called Fraud Guard and our own enterprise systems were not as advanced.[3] With Twilio, we have guaranteed quality."

SENIOR PROJECT SPECIALIST, RIDE-HAILING

Return on investment (ROI)	Benefits PV	Net present value (NPV)	Payback
174%	**$2.35M**	**$1.49M**	**<6 months**

Benefits (Three-Year)

Accelerated market expansion	$1.1M
Avoided loss from fraud	$909.6K
Reduced time for fraud prevention labor	$215.3K
Avoided downtime due to route optimization	$91.9K
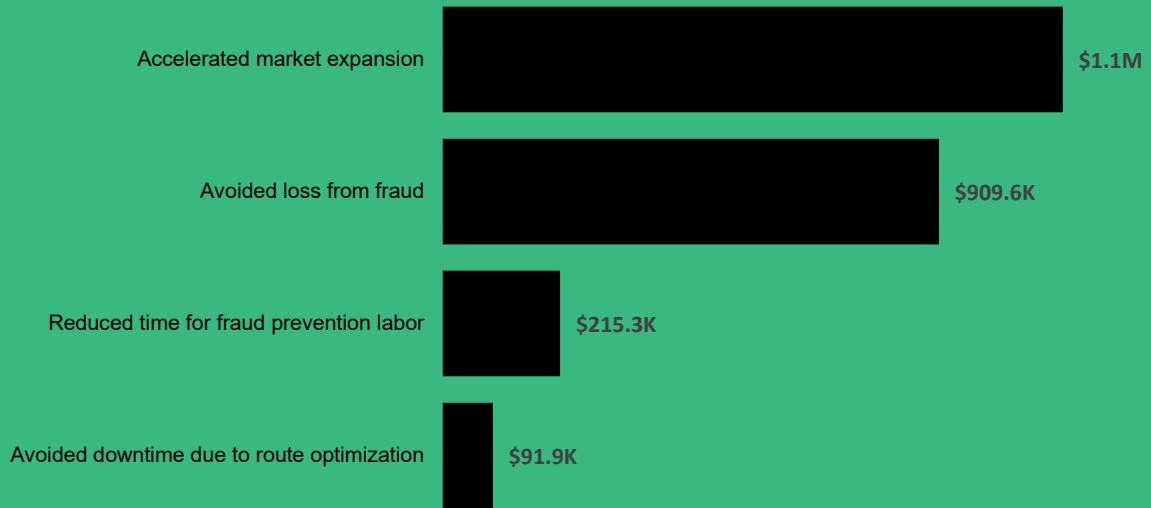
TEI FRAMEWORK AND METHODOLOGY

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

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 Verify can have on an organization.

DISCLOSURES

Readers should be aware of the following:

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

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

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

Twilio provided the customer names for the interviews but did not participate in the interviews.

1. Due Diligence
Interviewed Twilio stakeholders and Forrester analysts to gather data relative to Verify.

2. Interviews
Interviewed five representatives at organizations using Verify to obtain data about costs, benefits, and risks.

3. Composite Organization
Designed a composite organization based on characteristics of the interviewees' organizations.

4. 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.

5. 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 Twilio Verify Customer Journey

Drivers leading to the Verify investment

Interviews				
Role	**Industry**	**Region**	**Annual Revenue**	**Employees**
Senior project specialist	Ride-hailing	Headquartered in the US, global operations	$790 million	3,000 employees
Director of product	Video streaming platform	Headquartered in the US, global operations	$143 million	1,500 employees
• Product manager • Associate product manager	Sports technology and entertainment	Headquartered in the US	$3.29 billion	4,200 employees
Software engineering manager	Online food delivery	Headquartered in the UK	$2.42 billion	4,000 employees

KEY CHALLENGES

Interviewees' organizations faced challenges with fraudulent activity and abuse, difficulties in identifying and resolving issues due to limited visibility, and impediments in scaling operations globally. Prior solutions and processes included traditional SMS gateway or delivery systems that were vulnerable to fraudsters' tactics, resulting in distorted metrics, financial losses, and security risks. 2FA systems occasionally disrupted user flow and restricted end-user access. Insufficient resources and insights made it challenging to differentiate between legitimate and fraudulent activities, leading to delays and missed opportunities. Expanding globally involved navigating diverse regional regulations, connectivity issues, and cost implications.

The interviewees noted how their organizations struggled with common challenges, including:

- **Fraudulent activity and abuse including SMS pumping and promotion fraud.** Interviewees described that fraudulent activity and abuse in their prior environment were related to SMS pumping and fraudulent account opening or upgrading. SMS pumping — which involves fraudulent activity and abuse —

posed significant challenges as fraudsters constantly adapted their tactics and used advanced techniques and technologies to exploit vulnerabilities in SMS OTP end-user flows. Customers found it difficult to differentiate between legitimate and fraudulent traffic as fraudsters mimicked authentic end-user behavior. Customers who lacked awareness and education about SMS pumping in their prior environment faced increased risk of fraudulent activities impacting their business, which led to distorted metrics, financial losses, damage to reputation, negative end-user experiences, security risks, and regulatory or legal consequences.

The software engineering manager at an online food delivery organization commented: "We were experiencing this type of abuse where fraudsters were signing up for new accounts. We give promotions to new customers to get them onto our platform, so if there's multiple new accounts, it's hard to distinguish which ones are genuine and which ones belong to the same user or is a fake account."

- **Issues with standard messaging APIs used for 2FA.** Interviewees explained that prior environments involving standard messaging APIs used for 2FA occasionally experienced business disruptions due to the lack of built-in route optimization for sending OTPs. These disruptions resulted in serious implications for security, privacy, and user trust, and caused notable revenue loss. These disruptions weakened the overall security of accounts and prevented new users from creating accounts or performing activities on existing user accounts. The associate product manager at a sports technology and entertainment organization noted, "If we have issues with 2FA, it's a requirement to be able to access your account and log on, so end users would not be able to log on to their account. If they are already logged on but 2FA is down and they were trying to request a withdrawal change information on their account, they wouldn't be able to do so either. So, it is pretty restricting when we do have issues."

- **Difficulty identifying and resolving issues without proper insights.** Interviewees noted that identifying and resolving issues without proper insights to distinguish between legitimate and fraudulent activities in their prior environments led to an excess of false positive fraud alerts. The lack of sufficient FTEs

dedicated to reviewing false positive fraud alerts posed a significant challenge in ensuring accurate detection of fraudulent activities. This shortage resulted in delays, missed opportunities, and increased risk of allowing actual fraudulent transactions to go undetected.

The senior project specialist at a ride-hailing organization commented: "We had an alert system that would alert us if there was suspicious activity, but it needed a person to act on it. It was tough because there were many alerts daily and sometimes they were false positive alerts."

- **Challenges in scaling globally and expanding into new markets.** Expanding operations globally presented challenges for interviewees' organizations due to varying regional regulations, connectivity issues, cost implications, and end-user adoption. One of the main limitations is the need to comply with different regional regulations and compliance requirements for data protection and privacy. Each country and/or new market may have its own set of rules, making it complex and time-consuming for organizations to ensure their authentication solution aligned with these regulations.

  The director of product at an video streaming organization commented, "Verify was really an out-of-the-box solution that allowed us to globally expand multichannel authentications."

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Improve authentication in their digital platform.
- Block SMS fraud attempts.
- Optimize SMS messaging for optimized conversion.
- Expand into new markets.

"We went with Twilio Verify because we did not have to go and integrate in-house like every SMS provider carrier type. We are prepared for whatever else comes in the future — this becomes like a one-stop-shop for us."

DIRECTOR OF PRODUCT, VIDEO STREAMING

"The problems we were trying to circumvent were 2FA friction during the signup flow, and preventing users from creating multiple accounts using one email address. We decided to introduce Twilio Verify to prevent spam user accounts."

SOFTWARE ENGINEERING MANAGER, ONLINE FOOD DELIVERY

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 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 and deployment characteristics. The global, billion-dollar organization is headquartered in the US and has 4,000 employees. Prior to investing in Twilio Verify, the composite was using Twilio's Programmable Messaging for SMS 2FA. The organization has a high volume of SMS messaging resulting in a total of eight million SMS verifications annually. Twenty-three percent of these verifications are associated with fraud. Twilio Verify implementation is low effort and easily integrated with current systems in place, and is fully deployed over the course of a month.

Key Assumptions

$1 billion in annual revenue

4,000 employees

8 million total SMS verifications per year

23% of these verifications are associated with fraud

$0.05 per completed verification

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	Accelerated market expansion	$520,000	$440,000	$400,000	$1,360,000	$1,136,890
Btr	Avoided loss from fraud	$365,769	$365,769	$365,769	$1,097,307	$909,613 }
Ctr	Reduced time for fraud prevention labor	$86,569	$86,569	$86,569	$259,706	$215,284
Dtr	Avoided downtime due to route optimization	$36,955	$36,955	$36,955	$110,866	$91,903
	Total benefits (risk-adjusted)	$1,009,293	$929,293	$889,293	$2,827,880	$2,353,690

ACCELERATED MARKET EXPANSION

Evidence and data. Interviewees described how Twilio Verify helped their organizations enter new markets as a flexible and scalable multichannel authentication solution. With Twilio Verify, organizations could comply with regional regulations and privacy requirements, which is crucial when expanding into new markets. The platform also supports multiple languages and can be easily customized to cater to the linguistic and cultural preferences of different regions, ensuring a seamless end-user experience. Additionally, Twilio Verify offers various authentication channels beyond SMS, such as voice calls and push notifications. This allows organizations to reach end users in regions with limited internet connectivity or mobile network access, enabling a wider reach and end-user base.

- The product manager at a sports and technology and entertainment organization discussed the impact that Verify has on expanding their presence across the US, sharing: "Twilio helps us with our regional launches through emailing vendors with commissions, letting them know about what the business is and what they do, and getting their requirement for getting licensed for that state waived. If we don't get that waiver, we'd be blocked until they did."

- The director of product at an video streaming organization highlighted the impact that Twilio had on being able to enter new markets and being a leader in the space to grow globally. They noted: "When we were investigating solutions, Twilio was the only player that could help us enter new markets at a global scale. There weren't really any competitors."

- The product manager at a sports and technology and entertainment organization further highlighted the scalability and meeting of regulatory requirements with Twilio Verify. They shared, "With Verify, we are able to use short codes which allows us to scale our audience and also allows us to meet regulatory requirements and ensure that end users who are accessing the site are who they say they are."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- It has an annual revenue of $1 billion. With Twilio Verify, the annual revenue increases by 0.65% in Year 1, 0.55% in Year 2, and 0.50% in Year 3 as a result of entering new markets. The first year of new market revenue slightly declines over three years as the company penetrates the largest size and easiest markets first.

- Its profit margin is 10%.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Annual revenue.

- Profit margin.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.14 million.

0.65%

New market revenue in Year 1

"The fact that we grew to the size we grew in our new market was a huge win for us in terms of going from zero to thousands of customers."

DIRECTOR OF PRODUCT, VIDEO STREAMING

Accelerated Market Expansion					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Annual revenue	Composite	$1,000,000,000	$1,000,000,000	$1,000,000,000
A2	New market revenue	Interviews	0.65%	0.55%	0.50%
A3	Profit margin	Composite	10%	10%	10%
At	Accelerated market expansion	A1*A2*A3	$650,000	$550,000	$500,000
	Risk adjustment	↓ 20%			
Atr	Accelerated market expansion (risk-adjusted)		$520,000	$440,000	$400,000
	Three-year total: $1,360,000		**Three-year present value: $1,136,890**		

AVOIDED LOSS FROM FRAUD

Evidence and data. Interviewees described how Twilio Verify helped their organizations avoid losses from fraud by providing a robust and secure authentication solution. Implementing authentication through Twilio Verify added an extra layer of security to their end-user accounts which made it more difficult for fraudsters to gain unauthorized access. Moreover, interviewees highlighted that Twilio Verify provided real-time fraud monitoring and analytics capabilities. Organizations could monitor authentication attempts, detect suspicious patterns or anomalies, and take immediate action to mitigate potential fraudulent activities. This proactive approach prevented financial loss and protect end-user accounts from unauthorized access. By leveraging the robust security features and real-time monitoring capabilities of Twilio Verify, organizations can significantly reduce the risk of fraud, avoid financial losses, protect end-user accounts, and maintain the trust and confidence of their end users.

- Interviewees noted that they could verify the identity of end users through multiple channels (e.g., SMS, voice calls, or push authentications) and automatically block suspicious messages from being sent with Verify Fraud Guard which ultimately reduced the risk of fraudulent activities as fraudsters found it more difficult to bypass or intercept the authentication process.

- The associate product manager at a sports technology and entertainment organization highlighted the potential impact on end users without Twilio Verify's authentication. They shared: "Because of the areas on our product where we have 2FA as a requirement, such as changing of address, personal information, or large withdrawals, Twilio Verify helps with making sure that the funds aren't going to incorrect people. This helps protect our customers funds."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- There are eight million SMS verifications per year. Twenty-three percent of these verifications are associated with fraud with a 95% true positive rate.

- The weighted average cost of fraud per SMS verification is $0.23. This is reflective of the majority of fraud alerts are associated with the cost of fraudulent

SMS messaging, which is typically $0.05, and a small minority involving other types of fraud which cost closer to $1.00.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of verifications per year.
- Percentage of SMS verifications associated with fraud.
- Percentage of true SMS fraud alerts.
- Average cost of fraud per SMS verification.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $910,000.

23%

Percentage of SMS verifications associated with fraud

"With the help of Twilio Fraud Guard, we mitigate fraud, automatically block bad numbers, or prefixes so that we don't spend money on the fraudulent SMS."

SOFTWARE ENGINEERING MANAGER, ONLINE FOOD DELIVERY

Avoided Loss From Fraud					
Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	SMS verifications per year	Composite	8,000,000	8,000,000	8,000,000
B2	Percentage of SMS verifications associated with fraud	Composite	23%	23%	23%
B3	SMS fraud alerts	B1*B2	1,840,000	1,840,000	1,840,000
B4	Percentage of true SMS fraud alerts	Composite	95%	95%	95%
B5	Weighted average cost of fraud per SMS verification	Composite	$0.23	$0.23	$0.23
Bt	Avoided loss from fraud	B3*B4*B5	$406,410	$406,410	$406,410
	Risk adjustment	↓10%			
Btr	Avoided loss from fraud (risk-adjusted)		$365,769	$365,769	$365,769
	Three-year total: $1,097,307		Three-year present value: $909,613		

REDUCED TIME FOR FRAUD PREVENTION LABOR

Evidence and data. Interviewees discussed the impact of Twilio Verify to help automate various fraud prevention tasks, which ultimately reduced the need for manual labor and improved efficiency in detecting and preventing fraudulent activities. Twilio's real-time alerts allowed businesses to receive instant notifications and alerts when suspicious activities are detected. This enabled fraud prevention teams to respond quickly to potential threats, thus minimizing the risk of fraudulent transactions or activities. Twilio reduced the need for constant manual monitoring by automating the detection and notification process, which freed up labor resources for other tasks.

- The software engineering manager at an online food delivery organization highlighted their trust in Twilio and its impact on fraud prevention efforts. They shared, "We know that the traffic spike will be fixed by Twilio, so we don't have someone activating, investigating, or keeping a model, we know we're notified by Twilio if something is concerning."

- The associate product manager at a sports technology and entertainment organization highlighted: "We have a bunch of blocked countries for high risk

areas in our settings in addition to Fraud Guard. These features definitely have been helping us handle some of the volume of fraud alerts."

- The software engineering manager at an online food delivery organization highlighted features in Twilio Verify that provided greater visibility into different kinds of fraud that were not detected in their prior state with internal tools alone. They noted, "Twilio Verify has this functionality to implement other internal fraud controls that helps us connect users with each other so we can detect other types of frauds in the business."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- There are 10 fraud analyst FTEs who dedicate 10% of their time reacting to SMS fraud alerts.

- With Twilio Verify, time spent reacting to SMS fraud alerts fell by 95%.

- The average fully-burdened salary of a fraud analyst is $101,250.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of fraud analysts.

- Percentage of time spent by FTEs reacting to SMS fraud alerts.

- Average fully-burdened salary of a fraud analyst.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $215,000.

Reduced Time For Fraud Prevention Labor					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Fraud analyst FTEs	Composite	10	10	10
C2	Percentage of FTE time spent reacting to SMS fraud alerts	Composite	10%	10%	10%
C3	Percentage reduction in time reacting to SMS fraud alerts with Twilio Verify	Interviews	95%	95%	95%
C4	Average fully-burdened salary of a fraud analyst	TEI standard	$101,250	$101,250	$101,250
Ct	Reduced time for fraud prevention labor	C1*C2*C3*C4	$96,188	$96,188	$96,188
	Risk adjustment	↓10%			
Ctr	Reduced time for fraud prevention labor (risk-adjusted)		$86,569	$86,569	$86,569
	Three-year total: $259,706		**Three-year present value: $215,284**		

95%

Percentage reduction in time reacting to SMS fraud alerts with Twilio Verify

"We've reached a point where we don't have to worry so much about fraud."

SOFTWARE ENGINEERING MANAGER, ONLINE FOOD DELIVERY

AVOIDED DOWNTIME DUE TO ROUTE OPTIMIZATION

Evidence and data. Interviewees noted avoided downtime as a result of investing in Twilio Verify. Interviewees described a significant increase in uninterrupted business operations since replacing prior 2FA solutions, thus enabling a smoother workflow and increased productivity. Avoided downtime due to route optimization helped organizations maintain a positive reputation among end users. Furthermore, they reduced the risk of financial losses that could result from downtime, such as missed conversion opportunities or costly recovery efforts.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Prior to Twilio Verify, one significant 2FA disruption that resulted in two hours of downtime occurred annually.

- With Twilio Verify, downtime is reduced by 90%.

- The average hourly revenue is $200,000 and the operating margin is 10%.

- There are 12 software engineer FTEs who are involved in remediating 2FA disruptions. On average, they spend 10 hours investigating significant 2FA events to prevent them from happening again.

- The average fully-burdened hourly rate of a software engineer is $78. There is a 50% productivity recapture to account for reallocated time toward better employee experiences.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of 2FA disruptions per year and associated downtime per disruption.

- Average hourly revenue and operating margin.

- Number of software engineers needed to remediate 2FA disruptions.

- Time spent investigating significant 2FA disruptions.

- The average fully-burdened salary of a software engineer.

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 $92,000.

> "It's a requirement to be able to access your account and log on with 2FA, so when we had issues, end users would not be able to log on to their account. If they are already logged on and 2FA is down, they would not be able to request a withdrawal or change information on their account, so it is very restricting when we do have issues."
>
> **PRODUCT MANAGER, SPORTS TECHOLOGY AND ENTERTAINMENT**

UNQUANTIFIED BENEFITS

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

- **End-user satisfaction.** Interviewees highlighted the impact of Twilio Verify on protecting their end users as a result of improved fraud detection and prevention. End users entrust organizations with sensitive and personal data, and that can be detrimental if the proper steps are not in place to secure authentications. The associate product manager at a sports technology and entertainment organization commented: "Twilio provides our users comfort knowing that we take our security very seriously. The space is a very fragile space in general, and I think when you're talking about putting money into an account you want to make sure that your account is highly secure."

- **Integration with tech stack.** Interviewees discussed Twilio Verify's integration capabilities with various platforms and systems. It provides robust APIs that allow developers to easily integrate phone verification and authentication features into their applications. Twilio Verify also supports integration with popular programming languages, frameworks, and databases, making it easy to add verification functionality to existing systems. Additionally, it offers extensive documentation, code samples, and developer resources to simplify the integration process and ensure a smooth implementation.

> "With Twilio, we give customers reassurance that we take our security very seriously, especially in regard to regulatory requirements."
>
> ASSOCIATE PRODUCT MANAGER, SPORTS TECHNOLOGY AND ENTERTAINMENT

FLEXIBILITY

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

- **Avoided internal resources costs.** Interviewees highlighted the impact of Twilio's one-stop-shop solution to address their authentication needs rather than building a homegrown solution. By avoiding costs needed for infrastructure, time, and effort required for developing and maintaining a homegrown solution, interviewees' organizations are able to focus on its core competencies and other initiatives. Partnering with Twilio ensures organizations the access to specialized expertise, ongoing support, and continuous updates, which ultimately leads to improved functionality and security.

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

> "I think the core functionality of verifying that a code entered is the same one that was sent is time-consuming to build in-house. It would require a couple of months and several people's time to build internally."
>
> **SOFTWARE ENGINEERING MANAGER, ONLINE FOOD AND DELIVERY**

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
Etr	Licensing costs	$0	$323,400	$323,400	$323,400	$970,200	$804,248
Ftr	Implementation costs	$29,700	$0	$0	$0	$29,700	$29,700
Gtr	Ongoing management costs	$0	$10,098	$10,098	$10,098	$30,294	$25,112
	Total costs (risk-adjusted)	$29,700	$333,498	$333,498	$333,498	$1,030,194	$859,060

LICENSING COSTS

Evidence and data. Twilio Verify offers flexible pricing options based on usage and requirements. The licensing costs for Twilio Verify depend on factors such as the number of successful verifications, the country and region of the phone numbers used, and the volume of SMS or voice messages sent. Twilio Verify follows a pay-as-you-go model, where you only pay for the specific services and resources you use. Pricing may vary. Contact Twilio for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- There is an average of 6,160,000 completed verifications per year.

- Each completed verification costs $0.05.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Average number of completed verifications per year.
- Cost per completed verification.

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 $804,000.

Licensing Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Average number of completed verifications per year	B1-B3		6,160,000	6,160,000	6,160,000
E2	Cost per completed verification	E2		$0.05	$0.05	$0.05
Et	Licensing costs	E1*E2		$308,000	$308,000	$308,000
	Risk adjustment	↑5%				
Etr	Licensing costs (risk-adjusted)		$0	$323,400	$323,400	$323,400
	Three-year total: $970,200			Three-year present value: $804,248		

IMPLEMENTATION COSTS

Evidence and data. Interviewees highlighted a seamless implementation experience with Twilio Verify. Steps taken included obtaining API credentials, provisioning or verifying phone numbers to be used for verification purposes, and integration with Verify into the organization's application.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- Four software engineers spend 50% of their time in one month to implement Twilio Verify.

- The average fully-burdened monthly salary of a software engineer is $13,500.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Time spent by software engineers to implement Verify.

- Average fully-burdened monthly salary of a software engineer.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $30,000.

> "We completed implementation in one sprint or development cycle, which takes two weeks. For us, it was not very hard. It was just like adding another SMS filter and turning it on, so it was straightforward."
>
> SENIOR PROJECT SPECIALIST, RIDE-HAILING

Implementation Costs						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Months spent on implementation	Composite	1			
F2	Software engineers	Composite	4			
F3	Percentage of software engineer time spent on implementation	Composite	50%			
F4	Average fully-burdened monthly salary of a software engineer	TEI standard	$13,500			
Ft	Implementation costs	F1*F2*F3*F4	$27,000	$0	$0	$0
	Risk adjustment	↑10%				
Ftr	Implementation costs (risk-adjusted)		$29,700	$0	$0	$0
	Three-year total: $29,700		Three-year present value: $29,700			

ONGOING MANAGEMENT COSTS

Evidence and data. Interviewees highlighted that about 10% of a system administrator's time for ongoing management efforts were spent on maintaining the solution. This involved monitoring usage, performance, and security aspects of the Twilio Verify integration. Efficiencies in ongoing management were further improved by Twilio's robust monitoring and reporting tools to help organizations track and analyze the usage patterns and performance metrics.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- One system administrator spends 10% of their time on ongoing management of Twilio Verify.

- The average fully-burdened salary of a system administrator is $91,800.

Risks. Forrester recognizes that these results may not be representative of all experiences and that results will vary depending on the following factors:

- Number of system administrators.

- Time spent by system administrators on ongoing management.

- The fully-burdened salary of a system administrator.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $25,000.

Ongoing Management Costs						
Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	System administrators	Composite		1	1	1
G2	Percentage of system administrator time spent on ongoing management	Composite		10%	10%	10%
G3	Average fully-burdened salary of a system administrator	TEI standard		$91,800	$91,800	$91,800
Gt	Ongoing management costs	G1*G2*G3		$9,180	$9,180	$9,180
	Risk adjustment	↑10%				
Gtr	Ongoing management costs (risk-adjusted)		$0	$10,098	$10,098	$10,098
	Three-year total: $30,294			**Three-year present value: $25,112**		

Financial Summary

Consolidated Three-Year Risk-Adjusted Metrics

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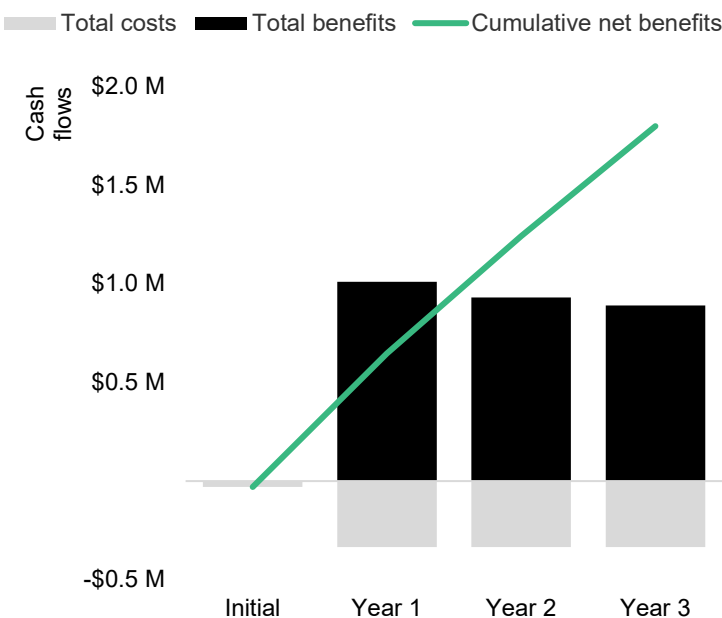
The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

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	($29,700)	($333,498)	($333,498)	($333,498)	($1,030,194)	($859,060)
Total benefits	$0	$1,009,293	$929,293	$889,293	$2,827,880	$2,353,690
Net benefits	($29,700)	$675,795	$595,795	$555,795	$1,797,686	$1,494,630
ROI						174%
Payback period						<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.

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.

APPENDIX B: ENDNOTES

---

[1] Source: [The State Of Decentralized Digital Identity (DDID): Key Use Cases And Adoption Trends](#), Forrester Research Inc., July 11, 2023.

[2] 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.

[3] Verify Fraud Guard uses automatic SMS fraud detection to block suspicious messages from being sent by your Verify Service. It works by analyzing your current and historical SMS traffic for unusual patterns. When it detects fluctuations in SMS destination traffic or SMS pumping fraud, Fraud Guard automatically blocks the prefix of the destination of the suspected fraud.