WHITEPAPER

Securing payments with Twilio programmable voice

TWILIO IS PCI DSS LEVEL 1 CERTIFIED

PCI STANDARDS OVERVIEW

- Build and Maintain Secure Network and Systems
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy
- Protect Cardholder Data

Credit card fraud is the most common form of identity theft, with over 14.2 million accounts exposed and fraud losses totaling $905 million in 2017, according to a report by the Federal Trade Commission (FTC)[1]. At Twilio, we understand with stakes this high, mitigating the risk of a potential security breach is paramount.

Twilio's Payment Card Industry Data Security Standard Level 1 (PCI DSS) compliance and certification extensively expands the scope of how customers can accelerate their business by using our trusted cloud communications platform and APIs. Twilio customers can capitalize on our certification to provide solutions that will enable them to securely capture credit card data over the phone using Twilio Programmable Voice. Whether you are already PCI compliant or building an application that requires PCI compliance, rely on Twilio to accept payment securely. Organizations, big and small, have access to the Twilio platform to accept payments over the phone with security built in and PCI DSS v3.2.1 certified.

The Payment Card Data Security Standard governs technical and operational requirements for managing cardholder data on a consistent basis globally. All entities processing, transmitting, or storing cardholder or sensitive authentication data must comply with this security standard or be subject to substantial financial penalties.

[1] *Source: Federal Trade Commission's 2017 Consumer Sentinel Network Report*

Accepting payments with Twilio Programmable Voice

Twilio's integration with payment providers eliminates the need for a business to become PCI DSS compliant to accept customer payments. Twilio will manage the capturing and processing of credit card information on your behalf using the payment provider of your choice.

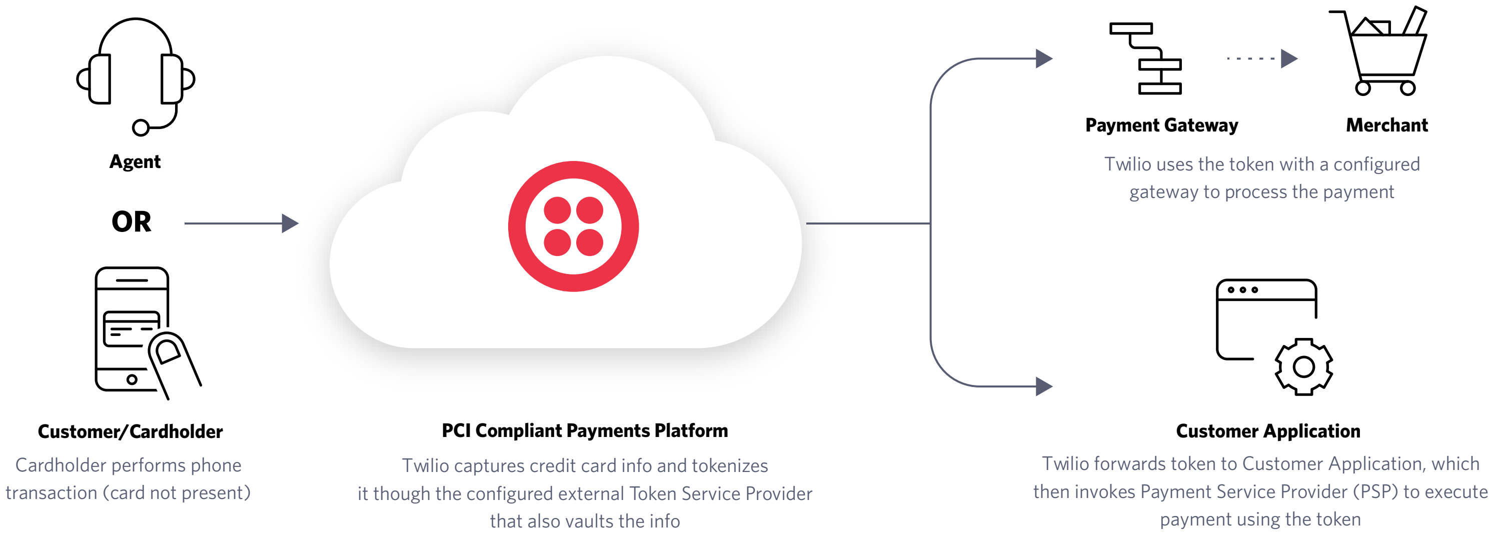
Self-Service Interactive Voice Response (IVR) is an intuitive and customizable automated pay-by-phone solution for collecting credit card information without an agent present. This minimizes our customers PCI compliance scope using our <Pay> API, that only requires one line of code, speeding your time to market and ultimately reducing your development costs.

Replacing payment card numbers with surrogate values (tokens) can be used in future payments without the need for the charging entity to access credit card information. Tokenization protects card data by substituting a card's Primary Account Number (PAN) with a unique, randomly-generated sequence of numbers. The generated number is the same length and format as the original PAN. Therefore, it is no different from a standard payment card number in the virtual eyes of back-end transaction processing systems, applications, and databases. This security technology is already being used by leading consumer financial brands like Visa and Mastercard.

Below, the diagram demonstrates how Twilio can be integrated on the front-end of the payment flow as a PCI compliant platform managing the collection and tokenization of credit card information or to optionally make a payment on behalf of customer applications. Payment gateways, used to authorize the transactions between you and your customer, can be selected from the Twilio Marketplace and support your existing billing relationships. In the case of executing the payment, Twilio would integrate with payment gateways classifying as card-not-present transactions, where neither the cardholder nor the credit card is physically present at the time of the transaction, which includes payments made over the phone.

The token is generated by the payment provider selected by the customer. Twilio is simply a proxy passing that information to the customer's application and will not store the information. Once a token is securely transmitted to the customer's application it is deleted. Payment providers can be selected from <Pay> Connector navigation link in the Programmable Voice console page.

Agent or Self-Service IVR


Agent

OR

Customer/Cardholder

Cardholder performs phone transaction (card not present)

PCI Compliant Payments Platform

Twilio captures credit card info and tokenizes it though the configured external Token Service Provider that also vaults the info

Payment Gateway

Merchant

Twilio uses the token with a configured gateway to process the payment

Customer Application

Twilio forwards token to Customer Application, which then invokes Payment Service Provider (PSP) to execute payment using the token

How Twilio Programmable Voice Complies with PCI DSS 3.2.1

Providing high levels of security is how we build trust in the tools our customers use to power their applications using our platform. Below is an overview of how Twilio is complying with PCI DSS standards.

- **Building and Maintaining Secure Network and Systems:** Developers must follow the Twilio Security Development Lifecycle (TSDL) while developing products, ensuring they are secure by design. Twilio's Cloud Security Standard (TCSS) comprises best-in-class security practices that include a defense-in-depth approach in our production environment, where all customer data and customer-facing applications are logically isolated in an AWS Virtual Private Cloud (VPC). Firewalls are used to maintain network segregation between different security zones in both the Corporate and Production environments. Twilio leverages AWS Access Control Lists (ACLs) to manage traffic and firewall rules are reviewed quarterly.

- **Protecting Cardholder Data:** Twilio supports TLS 1.2 to encrypt network traffic between the customer application and Twilio to safeguard sensitive cardholder data during transmission over open, public networks. Twilio defaults to the highest cipher supported by the customer's client; customers must enable TLS on their side. Twilio will never store cardholder data in our environment. Once the token is transmitted to the customer application the information is deleted via an automated process.

  Twilio employs a network-based intrusion detection system (IDS), GuardDuty, that analyzes AWS CloudTrail, VPC Flow Logs, and AWS DNS logs. It uses threat intelligence feeds, including lists of malicious IPs and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within the Twilio AWS environment.

- **Maintaining a Vulnerability Management Program:** In adherence to the Twilio Vulnerability Management Standard, scans are conducted periodically and target different segments of our infrastructure.

  Employee laptops have behavior-based anti-virus and anti-malware detection.

- **Regularly Monitoring and Testing Networks:** Twilio logs high risk actions and changes in our production network. We leverage automation to identify any deviation from our technical standards and raise issues within minutes of the configuration change occurring. Periodic risk assessments are performed at least annually to review the effectiveness of existing security controls and safeguards, as well as to identify new risk. Internal penetration testing is performed every six months to verify segmentation methods are operational, effective and the Cardholder Data Environment (CDE) is isolated.

- **Implementing Strong Access Control Measures:** Access to information is restricted with a least privilege model. Twilio employees must take Twilio Security and Privacy training once a year, which covers our information security policies, best practices, and privacy principles to support company-wide awareness on the importance of security.
- **Maintaining an Information Security Policy:** Twilio maintains a suite of information security policies and standards as part of our continued commitment to maintain the confidentiality, integrity, and availability of Twilio systems, customer confidence, and corporate governance. These policies and standards apply to all Twilio employees, interns, and contractors accessing internal systems and/or customer data.

We also provide developers with a library of resources to facilitate integrating Twilio into their applications with security available at https://www.twilio.com/docs/usage/security. Additionally developers can reach out to our support team 24/7.

Twilio's Trust Mission

Trust is Twilio's most important security principle. It is founded on bold transparency, shared responsibility with our customers on the security journey, and our holistic approach to design, development and deployment. Your trust in Twilio is our top priority. PCI DSS Certification aligns with Twilio's continued effort to build customers trust in us to grow, support, and revolutionize their business.

Click below to learn more about Twilio's PCI DSS Certification and resources to build your business payment needs.

Learn more