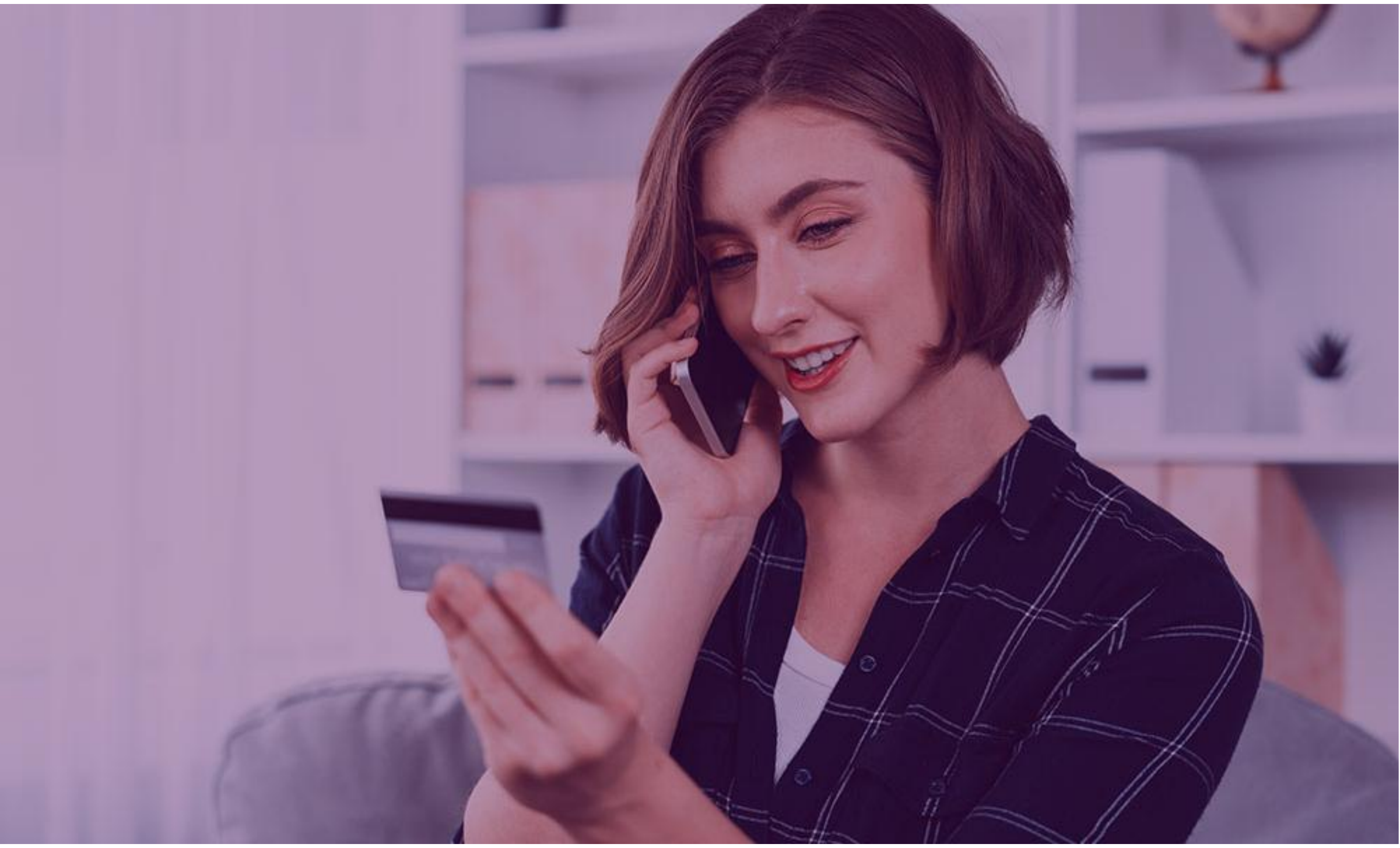
+44 (0) 1302 513 000
sales@keyivr.com
www.keyivr.com



Automated Payment Line

A fully automated payment collection system.

Provides secure, automated telephone payments using IVR. Callers enter card details directly, without agent involvement, allowing PCI-compliant self-service payments. Reduces call traffic and maintains a consistent, accessible customer experience.

Service Features

- DTMF-suppressed, voice or digital IVR payments
- Fully automated, agent-free payment capture
- Multi-language IVR prompts
- Configurable menus and call flows
- 24/7 availability for inbound payments
- Real-time payment confirmation
- Save details securely for future, repeated payments
- PCI-DSS aligned architecture
- Telephony platform integration
- Detailed call and transaction reporting

Service Benefits

- Enable customers to pay without speaking to an agent
- Reduce call handling time for contact centres
- Lower operational costs through automation
- Maintain PCI compliance without agent involvement
- Improve payment completion outside business hours
- Reduce queue times during peak periods
- Support accessible, self-service payments
- Minimise exposure to sensitive card data

Core Service

Automated Payment Line (Payment IVR)

A fully automated, 24/7 telephone payment service, allowing customers to provide sensitive card details using their telephone keypad in a PCI-compliant manner. The keypad entries are DTMF-suppressed and payments are processed as a MOTO transaction.

Upgrades are available to add additional payment options and data capture methods such as Voice and 3DS2 secured payment links.

Optional Upgrades

3DS2 ECOM

3DS2 is a secure online payment authentication protocol that verifies a customer's identity during a card-not-present (CNP) transaction to reduce fraud while minimising checkout friction.

In regard to an Automated Payment Line, Key IVR can send a payment link, rather than requesting the payment is processed via the user's telephone keypad. The customer will be advised that a link has been sent to them via Text message / SMS, and they will continue their payment journey online (ECOM). Key IVR provides 3 online payment methods during the checkout process:

- **Card Only:** Accepts debit or credit card payments – VISA, Mastercard and American Express.
- **Card & Digital Wallets:** Accepts the above, plus digital wallets including Google Pay and Apple Pay.
- **Card, Digital Wallets and Open Banking:** Accepts the above, plus adds bank to bank transfer options to your online payment journey. Receive funds straight away, free from any risk of chargebacks and card-not-present (CNP) fraud.

Agent Pass-off Capability

The customer will be on the phone with an agent discussing a payment. At the point a payment is required, the agent can verify the customer, enter the referencing details and the payment amount. The agent will then transfer the customer into the payment line, at which point the agent will no longer be on the phone.

The customer will be greeted by the automated voice prompts and will confirm the details the agent inputted previously. The customer will then key in their card details into the telephone keypad. The payment is then processed via the gateway, once complete the automated voice will read out the authorisation code, followed by an optional SMS receipt. If a customer struggles to make a payment, or the customer requires to speak to an advisor post payment, the solution can also redirect the customer back to the agent.

Voice IVR (using AI capture and transcription)

Using a telephone keypad to input account information or card details can be challenging for some customers, especially for those with a severe physical disability. It can also be important to capture non-numerical information from your customers, or a mix of alphanumeric – such as name, postcode, National Insurance number or car registration.

To cater for all demographics and information formats, our service can be configured to prompt the customer to speak details out loud, accurately deciphering their answers and progressing to the next step. Our AI technology uses grammar, syntax, structure, and composition of audio and voice signals to understand and process human speech.

Card details are verified and processed securely. The system will mute the call as sensitive details are spoken, so any call recordings are out-of-scope and you remain PCI-DSS compliant.

Language Pack - English (UK) already included

Ability for the IVR prompts to be in alternative languages, English (UK) is already included as standard. Below is a list of all languages currently available:

French (France)	English (Canada)
French (Canada)	English (Ireland)
German (Germany)	Portuguese (Portugal)
Italian (Italy)	Spanish (Latin)
English (US)	Spanish (Spain)

Tokenisation - Save payment details

Tokenise a customer's card, meaning they will only need to provide card details once, saving them time on regular payments and purchases.

All payments are secure as card details are not stored anywhere outside the issuing card company, with tokens containing a dedicated reference for every individual customer.

E.g. Policy number, customer number, customer name, phone number, etc

Recurring Payment Plans (Continuous Payment Authority)

Offer your customers a Recurring Payment Plan with a range of payment frequencies, such as weekly, fortnightly, monthly, etc.

A Recurring Payment Plan / CPA (Continuous Payment Authority) differs from a Direct Debit as you can re-take failed payments, restarting the plan and avoiding expensive failed payment charges.

This method is recommended by the FCA, as debt isn't added onto customers paying off existing debt.

Transfer Call to Contact Centre

The IVR can ask the customer if they want to be transferred to an agent. For example: After a payment has been made, if they need additional support or for additional reasons. Pricing varies depending on the phone number, details available in the Pricing Document.

Text Message / SMS and Email Receipt

Allow for customers to receive a Text Message / SMS and Email receipt of their transaction following the completion of a payment. The customer will be presented with it as an option at the end of the call. An optional extra to the service with only a cost per Text Message / SMS and Email – see Pricing Document.

Email receipts require an API integration.

Additional Project Management

As standard, 1 day of Project Management is included. For highly complex projects or projects that require additional resources, we charge a set day rate for additional Project Management. This includes remote and on-site visits.

Optional Integrations

You can automate the payment process either through an API integration or a partial integration using SFTP, improving reconciliation and enabling a more streamlined, automated workflow by reducing manual payment collection and reconciliation tasks.

SFTP (Upload of historical debt)

With the option to upload customer data, or a list of outstanding payments, transactions can be validated as a customer makes a payment. This information is picked up directly from our SFTP site, or alternatively you can host this within your own systems to be collected and uploaded automatically.

REST API

This pre-built API is ready to go and allows the Automated Payment Line to securely integrate with your systems, enabling automated control and exchange of payment and call data to streamline payment processing and reconciliation.

Bespoke API

Our solutions are compatible with many APIs, allowing integration with hundreds of different platforms. A bespoke API is developed to work seamlessly with your business systems 24/7. With a direct API Integration to your internal platform, we can correspond through a SOAP/Web Service, validating information as it is entered by the customer or agent.

By confirming reference numbers, identifiers and amounts, then posting information back into your CRM in real-time, you save valuable time with no manual reconciliation.

What are the requirements?

Our API integration connects to your organisation's or IT partner's endpoint using common SOAP, WSDL or REST technologies. We would liaise with your IT team to connect our payment solution with your systems. However, if you don't have available IT resource we are able to build both halves of the API integration.

PSP Connection

Key IVR Gateway Service

Using one of our white labelled gateway - quick onboarding, works with all major acquirers. An alternative to your existing gateway or a gateway we don't support.

Gateway Configuration (Existing API integration)

Use one of our existing PSP connections with leading gateways.

Adflex	Ecom 365	PayPal
Adyen	Elavon	PayPoint
ANZ	Fidelity Payments (Fidelipay)	PayPoint IMA
Axcess	FirstData	Paysafe
Barclaycard Advanced /	FiServ	Payzone
Smartpay Bureau	Global Iris	Pineapple payments (Fiserv)
Barclaycard Smartpay A	Global Payments	RealEx
Barclaycard Smartpay Fuse	GOV.UK Pay	RocketGate
Barclaycard EPDQ	Heartland	RSM2000
BarclayCard Fuse	Ingenico	Saferpay
Cardnet	Mastercard(TNS)	Secure Trading
Cardknox	Monek	Stripe
CardStream	NetBanx	TNS
Cashflow	Nexi	TotalProcessing
CenPos	Commidea	Transax
Checkout.com	CreditCall	UPG
Commidea	Cybersource	Vantiv
CreditCall	Commidea	Verifone
Cybersource	CreditCall	WorldLine
DataCash	Cybersource	WorldPay

New Gateway Integration

Building a new integration to a PSP for which we don't have an existing API integration for (see Gateway Configuration above).

Alternatively, the organisation can migrate to our own Key IVR Gateway Service.

Transactions

Transactions processed through the payment service are billed each month, depending on volume (see Pricing Document).

Information Security Policies & Processes

At Key IVR the security of our systems and solutions, and the protection of data entrusted to us by our clients and customers, is core to everything we do. The in-house security team works closely with all key business functions to ensure a stringent adherence to our constantly evolving information security polices and procedures is maintained.

Support spans across the business from Senior Management team members down through all team member levels. Our policies and processes have been developed in line with the following standards

- ISO27001 2022
- PCI DSS Version 4.01
- Cyber Essentials
- GDPR
- NCSC

Accreditations

Project Management

Our Team is here to ensure your project runs smoothly. They will assist your organisation with any information, training or queries you may have. Working closely with your Account Manager, they will ensure the delivery of your new service and keep a watchful eye on the platform that will protect every process to GDPR, ISO 27001 and PCI-DSS Level 1 standard.

Project Manager
Processes all documentation including specification and obtains approval for any upcoming work

Developer
Designs and builds the solution according to the specification

Quality Assessor
Thoroughly tests your new solution, ensuring everything is working how it should be

Customer Success Manager
Dependent on the project, the CSM may be involved for additional support throughout the process

Hypercare team
1 – 4 week process to closely monitor the success of the solution throughout the initial go-live period

1st Line Support team
Primary communication channel for anything system or data related

Account Manager
Responsibility of client communication and escalation will be returned back to your account manager

Project & Onboarding Process

Initiation & Planning

2. Contract
- Request raised (Dynamics)
- Requirements understood
- PO Initiated / Paid
- Impact Assessment

3. Initiation
- Project initiation meeting
- Project scope defined
- Technical requirement review
- Specification call
- Specification build
- Project plan initiated
- Project plan created
- Specification reviewed and signed off by client in writing

Execution

4. Build
- Tasks assigned to the development teams
- Development teams build & test to the specification requirements
- Release notes are generated
- The project manager manages updates to the customer, RAID log, project plan & customer actions log

5. Test
- Integration signed off by QA
- PM schedules in release to staging
- Solution successfully deployed by release team
- Regression testing in Staging environment
- Solution signed off in Staging environment by QA

Implementation & Closure

6. UAT
- Solution handover sent to client for a maximum of 2 weeks UAT
- Any issues raised on log resolved in bug fix and solution passed back to client to continue UAT
- PM prepares the go live delivery
- Client signs off solution in staging environment in writing and advises any external dependencies for customer live

7. UAT

- Release notes created and submitted for technical review
- Release Timeline
- Client Alignment
- Schedule rollout
    - Risks / Impacts captured
    - Live testing completed by QA
    - Release notes created and submitted for review
    - Technical review completed pre-release and approved
    - PM communicates scheduled release date to all parties once approved internally
    - Live testing completed by QA
    - Solution signed off in live environment by QA

8. Customer Live

- Transacting – client side
- Meets client requirements – client sign off
- Hypercare
- Service delivery handover
- Solution handed over to client to perform end to end test and sign off in writing
- Solution moved to billing
- Hypercare commences with client for 4 weeks managed by CEX & support teamsSolution completes hyper care, Moved to BAU with A/M and support

Fault Categories, Response and Resolution Times

Timescales for Resolution

Timescales for fault resolution will be measured from the point the original fault is reported to Key IVR up to resolution of the fault as confirmed by the client (unless otherwise specified).
NOTE: SLA response will be a helpdesk ticket opened and customer notified of the Priority level of ticket. i.e. Priority 3 email is sent to Key IVR @ 16:50 on a working day, response could be by 09:50 on the next working day.

Key IVR Priority Definitions

SLA Category	Description	Examples
Priority 1: Critical	Faults or incidents significantly affecting availability of the services being provided by the system.	· Total service unavailability · Failure of >=10% of transactions
Priority 2: High	Faults or incidents which affect service on an intermittent basis which significantly affects payment processing	· Failure of < 10% of transactions over a 1-hour period
Priority 3: Medium	Faults or incidents producing a minor impact. Problems specific to a non-core service or uncommon scenario.	· Inability to change processing options

Notes: SLA Category to be agreed between both parties, SLA category will not be changed without agreement from both parties.

Key IVR Incident Logging Process

Step	Action	Responsibility
1	Incident is reported to Key IVR's Service Desk	Client's Service Desk
2	Incident is recorded in Key IVR's ticket management system	Key IVR
3	Priority agreed	Key IVR & Client
4	Updates provided to the Client in accordance with the SLA schedule	Key IVR
5	Escalations to be conducted as per the agreed Escalation schedule	Key IVR
6	Incident resolution reported to the Client	Key IVR
7	Incident confirmed as resolved by all parties involved	Key IVR & Client
8	Call closed	Key IVR

Service Support Operating Hours

Method	Operating Hours
Telephone Support	08:30 - 17:00 Monday to Friday
Email Support	08:30 – 17:00 Monday to Friday

Out of Hours	Detail
Out of hours number	+44(0)1302 513000 option 1 Voicemail available emailed to on call team.
Out of office hours email responded to	Response by 10:00am the next working day

Key IVR Service Levels

SLA Category	Support Coverage	Response	Target Resolution	Target Communication
Priority 1: Critical	Monday to Friday, 0830 to 1700	5 minutes	3 hours	Every 1 hour
Priority 2: Medium	Monday to Friday, 0830 to 1700	60 minutes	8 hours	Every 2 hours
Priority 3: Low	Monday to Friday, 0830 to 1700	4 hours	5 working days	On request
Priority 1: Critical Out of hours	Monday to Friday 1700 to 0830 Saturday and Sunday 24*7	60 minutes	4 hours	Every 2 hours

Notes:

The client accepts that there are several components to service provision which are outside of the control of Key IVR.

Where a fault is agreed to lie outside of Key IVR responsibilities Key IVR will provide all reasonable assistance to assist the client and its associated parties to determine the root cause of the fault.

End-of-Contract & Offboarding

Customers may request a final export of their data. Data exports will be request through and completed by Key IVR. The exported date will be provided through a secure method such as an sFTP connection.

Once data has been successfully transferred and the service has ended, customer data is securely deleted in line with our information security and asset handling procedures.

About Key IVR

Key IVR is a privately owned business offering automated payment services across the globe. We are a customer-service focused organisation and take care to manage and meet our client's expectations.

Hosted in leading data centres and processing over £2 billion per annum, our state-of-the-art payment suite is robust, reliable and secure – certified to PCI-DSS v4.01 Level 1 by our QSA, LRQA Nettitude.

Available in 28 countries, 14 languages, and 11 currencies, our solutions are recommended by the Chartered Institute of Credit Management, worldwide payment gateways and PCI-DSS QSAs.

Our mission is to provide high-volume automated payment collections through great software and delivering excellent customer service. We aim to be the provider of choice for companies wanting to deliver high-quality payment collection systems to their clients and customers.

Visit www.keyivr.com to find out more