ePayments for Prisoners and Detainees in Secure Environments

1. Service Summary

Unilink's Secure Payment Service provides a safe, fast and secure way for friends and family to transfer funds to a prisoner or detainee using electronic payments via a secure website. The service is designed for use across prisons, secure hospitals, detention centres and secure training centres.

The service replaces cash, cheques and postal orders with a controlled digital payment process, improving security, traceability and operational efficiency. Payments are routed securely to the correct recipient account and deposited into a trusted institutional bank account through established card payment networks. Where establishments use a Unilink offender management solution, payment reconciliation is performed directly within the integrated finance module, providing end-to-end visibility from receipt through to allocation

Delivered as a UK-hosted, device-agnostic cloud service, Secure Payment Services reduce administrative effort for finance teams while providing a simple and accessible experience for external senders.

2. Service Features

The service provides a secure, managed payments capability, including:

- Payments delivered to recipient accounts quickly
- Senders register and log on to a secure website to submit payments
- Secure routing of payments to the correct prisoner or detainee account
- Payment receipts or notifications provided to senders
- Funds deposited into a trusted bank account via card payment networks
- Configurable daily, weekly and monthly recipient value limits
- Configurable daily, weekly and monthly limits on number of payments
- Full traceability of sender identity and transaction history
- Device-agnostic, UK cloud-hosted solution
- Dedicated customer support for senders and institutions

3. Service Benefits

The service delivers financial, operational and security benefits, including:

- Easy for friends and family to send money quickly
- Improved security through removal of cash handling
- Full traceability of senders and transactions
- Reduced cash on site and fewer banking collections
- Reduced effort clearing cheques and postal orders
- Lower administrative burden for finance teams
- Automated processing reduces fraud and error risk
- Improved reconciliation and audit readiness

- Low or no cost for institutions to operate
- Supports safer, more efficient custodial operations

4. Service Scope

The service covers the end-to-end processing of electronic payments from external senders to prisoners or detainees.

Friends and family access the secure website to register, submit payments and receive confirmation. Payments are processed electronically and routed to the appropriate recipient account, subject to configured limits and controls.

Finance and administrative staff use reports and audit data to reconcile payments and monitor activity in line with local financial procedures. Where Unilink offender management solutions are in use, payment reconciliation and allocation are managed directly within the integrated finance module, supporting streamlined processing and consistent financial control.

5. How the Service Works

External senders register on the Secure Payment Services website and submit payments using standard card payment methods. Sender details and transaction information are captured to ensure full traceability.

Payments are processed through established card payment networks and deposited into a trusted institutional bank account. Transactions are associated with the intended prisoner or detainee and made available for allocation in line with local finance processes.

Senders receive confirmation of successful payments or notification if a payment cannot be completed. All transactions are recorded centrally to support reconciliation, audit and reporting.

In establishments using Unilink offender management systems, approved payments are automatically made available within the finance module for reconciliation and allocation, reducing manual handling and supporting accurate, auditable financial processes.

6. Onboarding and Offboarding

6.1 Onboarding

Onboarding includes setup of establishments, bank account details, payment limits and reporting access. Staff users are provided with access to payment reports and support materials.

Typical onboarding timescales range from two to three weeks, depending on configuration and number of establishments.

6.2 Offboarding / exit management

Offboarding is managed in a controlled manner, including withdrawal of access and provision of transaction history and audit data in line with contractual and regulatory requirements

7. Support and Service Management

Incidents and service requests are managed in accordance with the agreed contractual service levels and the operational requirements of custodial environments.

Initial response times are within 1 hour.

Standard support hours are Monday to Friday, 8:00am–5:00pm (UK time). In recognition of the critical nature of custodial systems, High priority incidents are supported 24 hours a day, 365 days a year.

Support is delivered using an ITIL-aligned service management framework. All requests are logged through a central service desk and assessed by a triage function, which assigns priority and routes issues to the appropriate resolver group. Resolution is provided through structured 1st, 2nd and 3rd line support, with clear escalation procedures in place.

Customers are provided with a dedicated support portal and an assigned Business Account Manager, who provides ongoing service oversight, technical engagement and escalation support. Service performance and incident trends are reviewed through agreed governance processes.

Senders are assisted via a 24/7 AI enabled chatbot and customer support team.

8. Service Constraints and System Requirements

8.1 Service constraints

- Payment limits and rules are subject to local policy and regulation.
- Settlement times depend on card networks and institutional banking arrangements.

8.2 System requirements

- Secure internet access and a supported web browser for staff and senders.
- Secure connectivity to the hosting environment.
- Role-based access controls aligned to customer security policies.

9. Security and Compliance

The service is designed with security by design, including encrypted data transmission, full audit logging and traceability of all transactions. Payment processing is handled through accredited card payment networks.

Where Unilink provides the managed service, it operates within ISO 27001-certified information security controls and GDPR-compliant data handling practices.

10. Training

Training is provided for finance and administrative staff covering payment processing, reporting, reconciliation and exception handling. Training can be delivered remotely or on-site and is supported by user guidance materials

11. Ordering and Invoicing

This service is ordered via the Digital Marketplace in line with G-Cloud call-off procedures. Pricing is provided separately in the G-Cloud pricing document

12. Trial Service

A phased rollout or limited pilot can be provided to validate payment workflows and reporting prior to wider deployment.

