# Annotated Use Case--ePayment Addresses

## Publicly Discoverable ePayment Address(es)

**Publicly Discoverable ePayment Address(es) Part 1, ENROLLMENT**:

**Use Case Description**: ENROLLMENT *This use case should be considered as a work-in-progress, and must still be evaluated within the financial services community for issues such as liability, regulatory concerns, privacy, and business value. This use case is being posted to the wiki to obtain greater exposure within the IDESG community, and to encourage comments from the community regarding technical, standards, privacy, and usability issues that appear to be relevant."*

"OVERVIEW: In the face of mounting market shifts, new technologies, and regulations, financial institutions must look to new revenue sources. The growth in e-commerce, mobile commerce, and alternative providers adds urgency to that search. An important opportunity, that leverages the considerable FI investment in KYC infrastructure, is the establishment of a “neutrally positioned registry” of payment addresses. Known as the Greenlist® , it is an enabling technology for **Immediate** funds transfer and, on a larger scale, secure value exchange to support transactions in what is an increasingly internet-dominated global economy."

"DESCRIPTION: Part 1 - ENROLLMENT. Minimal API consisting of a secureXML interface that is split into two separate interfaces: Registration (Enrollment) and Query. Via a person’s financial institution, obtain and register an ePayment Address to a financial account at said institution that is rendered safe to be publicly discoverable by masking account numbers with routable identifiers that can only receive deposits. Aligned with Fair Information Practice Principles (FIPPs) of data minimization & use limitation principles, ‘live’ bank account information never leaves the bank. The registry is the trusted custodian of benign debit-blocked payment address identifiers.

**Use Case Category**: Trust/Assurance, Authentication, Interoperability, Privacy

**Contributors** : Richard O'Brien - Payment Pathways, Inc., Peter Tapling - Authentify, Inc., and Peter Gordon - FISGlobal & PayNet

### Use Case Details

**Actors**: 1) Authoritative Parties – Operators of Registries containing Personally Identifying Information (PII) linked to publicly discoverable account identifiers supplied by an accredited registrar on behalf of registrants who have enrolled in highest level of privacy protection for financial account identifiers.

2) Financial institutions are accredited as Identity Attribute Providers [Note 1] upon their acceptance of liability for the binding of PII to ePayment Address (es). FIs trust and stand behind their own KYC [Note 2] process.

> **Note 1:**
>
> A full solution will need to specify the trust framework and attribute query protocol, define the supported attributes and stand up the technology to support queries for the defined attributes via the specified protocol.

> **Note 2:**
>
> KYC: Know Your Customer

3) Relying Parties – Risk bearing institutions that transfer money on behalf of their clients/account-owners.

4) ePayment Networks – (or their assigns) provision account identifiers that mask or “tokenize” ePayment Addresses. This renders said ePayment addresses incapable of being automatically debited.

**Goals**: 1) Access trusted information to assure ePayment addresses of intended recipients of money transfers are true and mitigate risk of certain financial fraud attack vectors.

2) Fraud reduction which may imply cost reduction for the relying party.

3) Faster access to cash for money transfer recipients.

4) Viable business model for relying parties desiring to deliver instant non-repudiable money transfers.

**Assumptions**: 1) The relying party is a financial institution.

2) As the source and owner of the registrant data, the Identity Provider accepts legal liability for the accuracy of the registrant data.

3) The Authoritative Party is a custodian of the registrant data and is responsible for maintaining the accuracy and timely updating of data on behalf of all accredited Identity Providers.

4) Both the Authoritative Party and the Identity Providers share in transaction-based service fee revenue paid by relying parties. [Note 3]

> **Note 3:**
>
> This model presupposes that the Authoritative Party registry is not co-located with the FI Identity Provider. Both components come into play when a user authorizes his/her FI to publish PII to the registry. The user will need to be informed about which PII attributes are being published to the registry.

**Requirements**: Internet access device, portal software, identity information for the authorizing user.

**Process Flow**: 1) User learns of an offer to obtain a safe publicly discoverable ePayment address from his FI.

2) FI obtains user's permission to list sufficient personally identifying information to aid in the discovery of the user's listing in the registry.

3) User selects a unique identifier that one can always be remember when one wishes to receive electronic payments from friends or strangers.

4) Registry affirms that requested unique identifier is indeed unique. If not, user re-submits the request. [Note 4]

**Note 4:**

- The Registry at the Authoritative Party (or the FI) will need to provide functionality for the user to recover his/her chosen identifier if they forget it. If this is done at the Registry, it will necessitate an authentication step (user to Registry) which is not otherwise identified in this use case.
- The Registry will have to pass the final unique identifier to the FI so that the FI can associate account numbers with that Registry entry.

5) FI obtains a "mask" for an RT/ACH bank account number (a.k.a.: "UPIC") and/or a debit card's Personal Account Number (a.k.a.: "Tokenized PAN").

6) FI registers one or both of the account number masks linked to the user's unique identifier and PII.

**Success Scenario**: 1) Success, User is entered into database.

2) Relying Parties can access registered users' information.

3) Relying Parties present PII to sender to verify that this is the intended recipient of the transaction.

4) Relying Parties trust ePayment Addresses as true and can now send transfers that cannot be repudiated for lack of sender authorization – which is completely in the control of the sender.

5) Recipient's financial institution can post "good funds" directly to clients' accounts instantly upon receipt of transaction message because settlement is always guaranteed.

6) Identities of International transaction participants reported to regulators per Dodd-Frank Section 1073

**Error Conditions**: 1) Failure, GLID is not unique.

2) Failure, Missing required parameter.

3) User's PII not found – user wishes to be anonymous (note: no current mechanism to query user's PII).

4) ePayment Address not found - user status: HOLD (note: no current mechanism to query ePayment address).