Submission to NIST – July 22, 2011

Notice of Inquiry

National Strategy for Trusted Identity in Cyberspace

EXECUTIVE SUMMARY: Payment Pathways, Inc. (PPI) is based in Chicago and has an eight-year history of research and innovation at the intersection of three fields of study: Trusted Identity, Security, and Asset Transfers of payments and certified information. As a result, we have been awarded two U.S. Utility Patents that recognize the unique, valuable and non-obvious nature our inventions of a network of registries with a new identity attribute: the public electronic payment address(es).

Now is the right time to put theory into practice. Our response to the Notice of Inquiry is in two parts. Part 1 addresses the issue of governance of the steering group for the National Strategy for Trusted Identities in Cyberspace (NSTIC) and Part 2 explicitly states the case for business models that will allow companies such as Payment Pathways to play a role in the Identity Ecosystem.

One of the greatest opportunities we collectively have to improve NSTIC would be realized if the government understood that without private sector participation in the Identity Ecosystem there really isn't much of an ecosystem. And without viable business value propositions for the private sector there isn't likely to be much participation. The governance of the Greenlist registry explicitly recommended herein, justifies why such an extension to the basic NOI is important. The content in Part 2 is an amalgam of advice and guidance input from various industry stakeholders and shareholders of PPI. It includes a roadmap for establishing the foundation to introduce, govern and implement the management of this new identity attribute so it can achieve widespread usage.

ORGANIZATION: Throughout this document, we attempt to explain what would happen were we to play a role in NSTIC and apply the work product we have completed thus far. Topics in the Part 1 table are revisited in various sections of the Part 2 narrative to relax the tension of having two parts in the response.

OVERVIEW: This document is the Payment Pathways–led response to the Department of Commerce's comprehensive review of governance models for a governance body to administer the processes for policy and standards adoption for the Identity Ecosystem Framework in accordance with the National Strategy for Trusted Identities in Cyberspace (NSTIC). We, and like-minded institutions, are participating in general, because:

- Data breaches and information compromises have exploded for online and card-not-present payments in recent years.
- We representatives of industry recognize that we must work together with banks to try to elicit actionable solutions to this growing problem.
- Banks and other risk-bearing institutions will learn about the benefits of our patented, privacy enhancing technology: GREENLIST.®

TO: NATIONAL INSTITUTE OF STANDARDS

RE: RECOMMENDATIONS FOR CONSIDERATION:

a.) Governance recommendation for Greenlist and the importance of its relationship to NSTIC

b.) Governance recommendation for the NSTIC

FROM: **PAYMENT PATHWAYS COALITION**
200 S. WACKER DRIVE, 15TH. FL.
CHICAGO, IL 60606
+1-312-346-9400
ROBRIEN@PAYMENTPATHWAYS.COM
HTTP://WWW.PAYMENTPATHWAYS.COM

PART 1. PPI'S RESPONSE TO NIST'S NOI:

Issues	Structure & Functions	Suggested Stakeholders
Leadership	Structure: Common Development & Distribution License Functions: • source code maintenance • potential for zero royalty licensing	Payment Pathways, Inc.'s Board of Directors in conjunction with its successor organization, the Governing "steering group" body for the National Strategy for Trusted Identity in Cyberspace"
Representation of Ecosystem participants	Neutral governance: by-laws and (TBD) defined rules of operation	50% non-bank financial institutions 50% banks and their regulators
Accountability measures	To the rules-making, governing bodies for the regulated banking industry's payment networks	NACHA and equivalent organizations in EMEA, Asia and elsewhere
Liability issues	NIST: Designation of the framework's assignment to all registrars of a consistent responsibility for liability related to key identity attributes NACHA: Operating Rules for regulated registrars OTHER (TBD): Operating Rules for non-regulated registrars	Banks, Skype, Google, etc. Consortia: Kantara, OIX, etc.
Accreditation and certification processes	Determine consistent, minimum accreditation rules for heavily regulated and lightly regulated	Banks, Skype, Google, etc. or their designated representatives, (i.e. NACHA, European Payments

	registrars alike Certify, accept and maintain all registrar accreditation	Council, etc.)
Cross-sector and cross-industry issues	Determine registrar liability for accuracy of asset transfer addresses Interface with Government regulators and standards bodies	Banks, Skype, Google, etc.
Balance of self-interested and self-regulatory roles of steering group participants	Not in scope of this document	Not in scope of this document
Adherence to Guiding Principles	This communication highlights for emphasis the following Guiding Principles in FIPPS: Security, Use Limitation	Steering Committee / Governance body
Interaction and involvement with standards development organizations and other technical bodies	NACHA – ACH Rules EFT Networks – EFT Rules W3C, NIST, E.C. various standards organizations	Steering Committee / Governance body
Use, development, and maintenance of a trustmark scheme	Greenlist trademark is registered in the U.S., E.U., China and India. It is proposed to NIST for consideration to label the registry of safe, publicly discoverable electronic payment addresses	Steering Committee / Governance body
The relationship of the steering group to the Federal Government	We suggest it should follow the model of the European Payments Council to the European Union	Steering Committee / Governance body
Interactions with international governments and fora	Visited the following stakeholders in preparation of this document: US: Fed. Reserve Bank of Atlanta, NACHA, Herndon, VA The Clearinghouse, NYC PULSE, Div. of Disc. Fin. Svcs. CashEdge, NYC NYCE, Division of FIS Banca d'Italia	Steering Committee / Governance body

PART 2. WHAT IS GREENLIST AND HOW DOES IT ENHANCE PRIVACY?

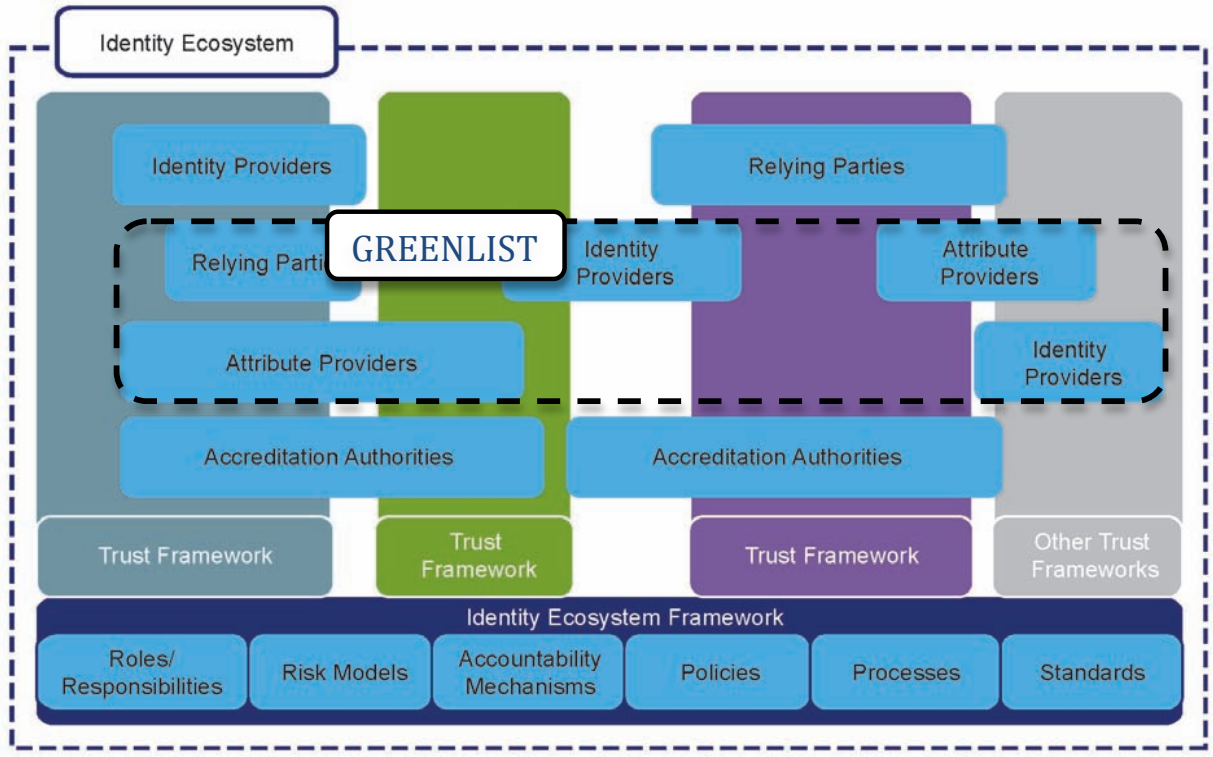
GREENLIST is a registry service for electronic payment addresses and is operated as a secure Web service for banks. GREENLIST uses state-of-the-art database and

security technology to verify that each party to a transaction is properly credentialed, based on easy-to-remember public identifiers such as an email address or other nickname. GREENLIST is available immediately for adoption by banks and payment, payment service providers and payment gateways.

There is nothing like this in the e-payments space; until now, e-pay users would have to track down a payees account, obtain routing numbers and reveal their own payment and account information. Passing that information back and forth is a risk many consumers and businesses recognize and choose to avoid.

As a secure alternative, the e-payment GREENLIST provides the user with a way to locate the virtual listing for payment addresses just as a "white pages" finds phone numbers and physical addresses. The difference is that the GREENLIST entry is only a pointer securely keyed to the actual accounts and routing information. It publicly exposes the bare minimum of information: the payment addresses that can only receive deposits to bank accounts. Consumers' real bank account numbers never have to be divulged to merchants or payment processor networks.

WHERE GREENLIST RESIDES IN THE NSTIC MAP



WHY WE PROPOSE A SEPARATE GOVERNANCE RECOMMENDATION *for Sub-Part "Greenlist:"*

As the graphic shows, Greenlisting does not just serve a particular Identity Attribute to be used on a particular money transfer network. Its function as *the* resource for an important, trusted identity attributes could potentially span several different Trust Frameworks. This neutral positioning accomplishes interoperability.

Payment ubiquity is an important guiding principle that NSTIC's governance candidates must protect.

Therefore, we recommend that the steering group responsible for governance should be drawn equally from three distinct groups, equally representing: a.) lightly regulated industries – Skype, Google, Western Union and the like; b.) heavily regulated industries – banks and the networks that serve the banking industry; and c.) standards, regulator and legislative governmental groups. Commercial and bank groups have a wide range of economic incentives to register proposed new identity attributes linked with a minimal set of public Identity Attributes to guarantee uniqueness. The new attribute is based on privacy enhancement technology required to create the safe, trusted, public ePayment address to be used to receive transfers of monetary and certifiably valuable information assets.

The reason why such a steering committee needs to encompass both lightly and heavily regulated groups is subtle; experience in Europe has proven that the open approach including lightly regulated entities in steering group is necessary to spur banks, a highly regulated and traditionally slow moving industry, into action.

BACKGROUND

The Internet has become a basic human right – right to hear, a right to speak and a right to be safely used. We now must define the conditions – when, where and how – privacy and safety are to be brought together. This must be done for *certain* Informational Transfer use cases and *every* Monetary Asset Transfer use case. Who should deliver those principles, and why?

Cash is the payment method of choice when anonymity is the objective. Sending and receiving electronic payments with speed, convenience and safety are the common objectives of banks, their customers and governments.

PROBLEM

Just as you don't want context information delivered to your social graph when you search because you don't want to be spied on, you also don't want items you purchase or sell (with the assumption of anonymity) – context information – being delivered without your permission. You have a right to expect that your bank account or debit card number (or other non-bank, de-coupled payment mechanism) can never be debited against your wishes. Such is the underlying premise of cardholder and accountholder agreements everywhere.

The quantity and variety of account number and card compromise threats from man-in-the-middle, man-in-the browser, key logging, memory imprinting and even spurious application attacks are especially extreme and often unabated at the level of the user's mobile device. The likelihood of account number and card compromise multiplies exponentially when private account data is at rest. This is often the case in today's payment market where private account data resides at numerous locations: mobile device as well as merchant and payment network locations.

Today's system of extreme caution to protect bankcard numbers with PCI Compliant storage protection at every merchant and every payment processor has become unwieldy and ineffective. Breaches of security continually outpace the market's ability to protect. The *only* effective safeguard is to *never* divulge an automatically *debitable* account number for electronic payment applications. Today, we consumers blindly provide dual purpose (debit and credit attributes in a single account number) payment account identifiers for a single purpose application. This is done for either application: paying or wishing to receive a payment. Consumers falsely assume that information will not be stored for possible re-use. This is done every time we write a check, every time we pay with PayPal, every time we use a bankcard that has not been Greenlisted. We make payments with an explicit context with an expectation of scope. We make payments with account numbers that have MORE Identity Attributes than are minimally necessary to accomplish the job of moving money. Banks have balked at teaching their customers any other method.

FIGHT FOR A NEUTRAL INTERNET AND NEUTRAL PAYMENT NETWORKS.

The more people that abuse the Internet, the more governments will try to take control of it. Anonymity is a fundamental right. It is a right to be left alone, not a privilege. A right to privacy – sharing data in an explicit context with an expectation of scope is as important as free speech. Sometimes these rights are in contradiction with each other. There are many places where anonymity is inappropriate.

For example, anomalous movement of large sums of money or large quantities of small transactions can be an indicator of terrorist cell activity. There is a difference from being spied upon and having a software system monitor your bank account's activity and alerting your bank whenever it exceeds historical norms. But account hijackers are clever. They know to use many different payment networks to aggregate and disperse funds. Only a neutrally positioned registry, an 'identity attribute switch,' can perform the canary-in-the-coalmine function to alert banks to further investigate suspicious activity and inform law enforcement officials when the needs for intervention or countermeasures arise.

PRIORITIES FOR THE GREENLIST ROADMAP

This Roadmap identifies the actions to be completed by all stakeholders (US and state regulator authorities, industry and users) over the next three years, following six priorities:

(1) Foster migration – to safer electronic payment addresses for specific purposes;
(2) Increase awareness and promote GREENLIST products;
(3) Design a sound legal environment and ensure compliance;
(4) Promote innovation
(5) Achieve standardization and interoperability; and
(6) Clarify and improve GREENLIST project governance.

FOSTER MIGRATION

Migration starts when the first GREENLIST Credit ACH and Credit EFT transaction products appear on the market and ends when GREENLIST products have replaced the

corresponding Debit ACH payment products and standards where desirable.
As GREENLIST comes online, banks will continue to run legacy debit payment applications while introducing GREENLIST protected credit payment applications in parallel. It is natural for banks and customers to determine those cases where credit payments are desirable. Therefore, migration should first be offered for the most desirable payment applications – those that enhance User Experience and contribute the most net new income to banks. The substantial benefits of GREENLIST will only materialize with rapid migration and the active commitment of both the demand and supply sides. While banks must of course offer high quality GREENLIST products, for rapid migration the following additional conditions must be met:

- **An Active Role for Public Authorities**
  With nearly 50 % of U.S. GDP and around 20 % of all cashless payments made, the public sector should play a leading role in GREENLIST migration. Together with other major players such as utilities, telecoms and insurers, public authorities can create the critical mass needed to speed-up migration.

  Through swift migration, public administrations can benefit from a streamlined procedure for payments, greater competition, and, a wider choice of payment service providers with prices reflecting improved economies of scale for payment processing. GREENLIST should also be integrated into the ongoing e-government projects. However, this is conditional on industry providing high quality and competitive GREENLIST products.

  Public authorities should draw up integrated and synchronized national migration plans, demonstrating their willingness to swiftly reach critical mass and drive forward the migration process. In addition, given Payment Pathways' crucial role, the existing governance arrangements of PPI deserve special attention.

- **Involving New Stakeholders – Increasing Visibility of the Issue**
  PPI has made progress in balancing the interests of different stakeholders, but it must operate in a more open manner to avoid possible reversal of its progress toward systemic change among banks (a.k.a. the foreclosure effect) and take into account the interests of all stakeholders, including non-banking stakeholders, payment institutions and users. The planning and design of future initiatives must ensure greater transparency, adequate time for consultation and early involvement of all stakeholders, in particular users.

Greenlist Relationship with Identity Consortia
Payment Pathways, Inc. is in communication with individuals representing organizations having stakeholder positions in Open Identity Exchange (OIX), OpenID, and the Kantara Initiative in the United States and the Electronic Payments Council (EPC) in Europe. While the EPC is the coordination and decision-making body of the European banking industry in relation to payments, its concerns extend into identity attributes. Unlike NACHA, the rules-making, governing body of the Federal Reserve Bank's ACH network,

the EPC's steering committee includes non-bank institutions. The broad base of its stakeholders defines its broader scope.

Action	Actors	Suggested Deadline
Establishment of effective Greenlist governance at the international level	E.C./ECB; US Dept. Of Commerce/NIST/NACHA	End-2011
Biannual reporting of progress in the implementation of the Greenlist Framework for action	Greenlist governance structure	From the date of establishment of the new Greenlist governance structure
Adoption of measures to the existing Greenlist governance model: 1) enhance stakeholder participation and consultation; 2) Increase transparency 3) Enlarge membership to payment institutions	NACHA	End-2011 End-2011 Nov.-2011
1) Evaluation of Greenlist governance structure	NIST/NACHA	End 2012

The Facebook page in Egypt, and the groups that started from it, were taken down because they were established anonymously. The right to be anonymous is a mechanism for blowing whistles. Anonymity is a high value card to be played and there is a very tricky balance between privacy and anonymity. We need to develop social institutions to create that balance.

Historically, electronic payment addresses were regarded as a privilege, not a right. Once upon a time, banks were the only institutions that were trusted to electronically move and safely store monetary assets. Today, there are many payment services that map unique identifiers to payment addresses. They range from email address-based PayPal to Kenya's M-PESA that uses the mobile phone number. Generally, multiple options exist in most parts of the world. Microsoft is poised to extend Skype by supporting new identity attributes.

What should be the relationship between the network and governance of that network (and registry)? What body defines the purpose specification that determines when and how context information pertaining to payments can be obtained and how long can it be stored?

GREENLIST, the patented registry for safe electronic payment addresses, would benefit to have guidance from the NSTIC stakeholders[1] to establish its governance structure.

RECOMMENDATION

Security through Use limitation through Data minimization – applications should only collect Personal Identifying Information (PII) that is directly relevant and necessary to accomplish the specified purpose and only retain PII for as long as is necessary to fulfill the specified purpose.

The Patriot Act requires checking the ownership of international payment addresses against the "do not send" list of known criminals and countries that support them. The steering committee will develop the policy framework that determines which entities get to query and retain *all* Greenlisted identity attributes.

Everybody who is on the Internet is in a country. If you're doing something fraudulent, you go to jail.

THEME – ROBUSTNESS:

Could big company or government cause the next big outage? Will it be like the New York power outage? Is there an unseen tipping point where one tweet can break it? Are we building a stable system? We need to make critical mobile web apps (like payments) more resilient. We're building Greenlist so HTTP-based query-search starts to morph into a peer-to-peer protocol seamlessly…if a tornado hits New York, will there be enough multiple copies of payment registries, etc?

Robustness has been increasingly more important since Haiti was devastated and the Tsunami hit the coast of Sendai, Japan. Both FEMA and HSA could justify roles for governance of Greenlist registries as a measure of protection of public safety. The Greenlist's neutral open systems framework allows for reaching where economic conditions vary. That is why mobile communication is effective.

THE CASE FOR LIGHTLY REGULATED INDUSTRIES AMONG STAKEHOLDERS IN GOVERNANCE:

The world still operates under a governance system that was built before we became a globally connected village where commercial enterprises launch services that frequently serve multiple cultures. How can we build a different topology?
Leaders at the recent Consumer Electronics Show (CES) said, "No one company can do it alone." All companies, large and small, are part of the Internet. Consumers have more choices. Institutions constantly find themselves racing to catch up and learn the steadily improving and changing technologies in the Information & Communications Technology space. It is simply not the old pattern anymore. We get new innovations and they die down or get adopted widely, and we continue on, always open to search and discover something new to try if we suspect our user

[1] Governments, Commissions, Regulators, Banks, and the Rule-Making bodies of various Payment Networks

experience could be improved. New innovations continuously happen. We cannot wait any longer for the banks to come up with a systemic global solution by themselves. We need to encourage today's registry exemplars to improve upon yesterday's level of service. Regular, access to trusted identity information and electronic asset transfer services need to be platform independent and universally accessible, anytime just as it can be from anywhere…even as far away as Canberra, Chongqing or Cadiz.

Multi-stakeholder approach is fraying at the edges. The fundamental problem is that evolution of jurisdiction and policy is built on an assumption of national sovereignty.

For instance, Skype's virtual service contract is based on Luxembourg law. This shows how a commercial stakeholder operating at scale is capable of acting beyond the realm of government policies. Skype repatriates money back to the United States. Skype, not government, determines how this gets done. Intermodal competition at the network access level defines how real gains happen in higher layers of the OSI model – especially in the application layer of 'the stack.'

DEFINITION OF SUCCESS:
What success looks like at Application Layer is maximum competition. For example, Universal Service Reform Effort is opening up access to networks to achieve the ubiquitous broadband network. Unlike net neutrality, there is much less public involvement in how subsidies are parsed out to smaller rural phone companies. This is important if we are going to have a ubiquitous broadband Internet. At the Application Layer, making mobile payments safe and private should be the concern of every bank in the world. Easy-to-use and efficient mobile payments should *not* only be offered the larger banks. Easy-to-use and efficient mobile payments should *not* necessarily only be offered by banks at all. Banks however, are centrally positioned since automated payrolls are sent to consumers' banks. Despite being potentially the most efficient electronic funds transfer agents, banks are very slow to create applications that encourage the migration of payments to electronics.

Banks have yet to choose an open and flexible architectural framework for public payment address registries that accommodate both banks and commercially successful non-bank payment service providers alike.

How we frame the problem determines how we solve it. Should innovation be done at network endpoints? Will banks redefine their traditional boundaries to encompass bank applications resident on their customer's mobile device? Banks must learn their role to educate their customers about how "the cloud" is becoming one's personal transactional memory.

"Banks must evolve beyond offering payment services for their customers and offer information delivery and storage services as a certified repository. If not doing anything, banks risk leaving an empty space for others to service."

Harry Leinonen
Advisor to the Board, Financial Markets and Statistics
Bank of Finland / Finland Ministry of Finance

Can both banks and non-bank identity attribute providers such as payment service providers innovate without restraint? Or do we want to innovate down the stack? There is a continuous disruption stabilization cycle. Low barriers for entry combined with venture capital, create many unmanageable designs. But such designs can be quickly scaled when proven to be successful. Mobile payments are a good example of commercial activity that runs ahead of regulators.

The Internet is a mass-market retail service by wire or radio that provides the capability to transmit data and receive data from all or substantially all Internet end points. Everything else is a means to an end. The endpoint is any protocol or Application Programming Interface (API).

GOVERNANCE OUTCOME DETERMINES USER EXPERIENCE:
Greenlist is about how consumers can experience the Internet in new, safer ways. Consumers know they have the ability to go anywhere they want to on the web, from anywhere they happen to be in the physical world. The most important word is radio. Thanks to Internet, the distinction between fixed line and wireless has blurred. Very soon money transfers may be on an unlicensed wireless network and a 4G licensed network and span multiple services across multiple payment networks in between. Rules must be harmonized for fixed line and wireless so public identity attributes for electronic payment addresses can be understood and demanded by consumers.

It is a primary objective of governance to encourage advancement of payments by accelerating the migration to electronics thru better latency. Tightly integrated apps improve user experience. Today, driven by Apple or Google, the whole environment is collaborative. We just have to make it get to the consumer. Banks, where AML and KYC and TRUST reside, are just the starting point. Competition between banks and non-bank payment service providers is healthy. It spurs the banks onward to defend their natural franchise in electronic payments.

SAFEGUARDING AN ARCHETECTURAL FRAMEWORK'S STABILITY:
There has to be a stable, neutral, non-competitive, and open "information hiding layer." Security professionals call this kind of solution, "cloaking technology." Whatever the word – hiding, cloaking, or masking – GREENLIST, like the Domain Name System (DNS), has to be kept open – not impeded by implementation of policy responses! (e.g. the recent effects of the Durbin Amendment to Dodd Frank Financial Reform Act of 2010)

The following lists the effects of the Durbin Amendment on the GREENLIST model:

- Banks less than $10B in Assets are not affected by flat-rate regulations for debit card fees… …except in case where de-coupled debit products are offered via directly or via third party commercial customers. This has triggered the withdrawal of Tempo from the marketplace, abandoning seven or eight large merchants and hundreds of thousands of consumers.

- Banks larger than $10B in Assets are now seeking new sources of non-interest income. Chase, Bank of America and Wells Fargo announced a P2P payment offering, based on a back office exchange of consumer database information, called ClearXchange, potentially affecting 49% of all US bank accounts.
- In direct response to ClearXchange, Fiserv (500+ banks – ZashPay) purchased CashEdge (200+banks – POPMoney)
- CashEdge and NYCE announced an instant P2P payment offering built upon the private registry of POPMoney accountholders.

Each of the aforementioned bank-centric service offerings are sub-optimal in nature because consumers are required to respond to email or text messages that announce to them that there is money waiting for them to retrieve. To receive the money the consumer is required to submit his bank account information.

The proper way to safeguard the public from account hijacking and other fraudulent threats is to guarantee stability at the interface. Control is the word. Standardization is the mechanism. When it comes to the automatic debiting and crediting of payment addresses, splitting today's debit/credit address into two separate addresses is simply the ONLY way to insure that addresses are not copied and stored longer than necessary to accomplish the task. The longer payment addresses are stored, the greater the vulnerability to outside hacking or inside employee malfeasance.

GREENLIST & INTERNET ARE CONSIDERED TO BE A COMMONS, LIKE OCEANS AND RADIO SPECTRUM:
Like environmentalism, protection of GREENLIST and Internet is not a political issue. Misappropriation of one's identity attributes harms rich and poor alike. Poorer people spend an disproportionate time trying to save money, for instance, paying a bill just in time at a Walmart store. They often pay more for transactions that are inherently riskier.

Research shows consumers understand the benefits of simple, automatic double-checking mechanisms to safeguard recurring payment instructions. Such techniques extend the use of the credit-only payment addresses into the realm of spontaneous bill presentment / bill payment – only after extra factors authorize the automated payment.

REMOVING BARRIERS FOR BANKS TO ACT:
Citizens need to engage more in regulations. Privacy, online safety, and cyber-security concerns affect the choice of technologies that need to be deployed. Privacy needs to be tackled well. Banks and the other non-bank entities that become accredited registrars to GREENLIST are correct to be concerned how this Payment Pathways' 'cloaking technology' could be licensed, administered and evolved from this point forward. Regulated stakeholders and non-regulated stakeholders alike

need to be involved in this important issue because it of its potential for positive systemic change.

Events we strive to support:

a.) The governance 'steering group' of NSTIC is formally constituted.

b.) The steering group defines an accreditation requirement and approval process for Greenlist registrars that other governing bodies can adapt without diminishing the level of trust that interoperable, universal service requires.

c.) NIST's staff identifies the Greenlist's framework for creating and managing an important new Identity Attribute as filling a present gap in the spectrum of *necessary* Identity Attributes.

d.) W3C designates Greenlist's XML enrollment and lookup libraries among its emerging application layer standards to the development community.

It is anticipated that NIST staff will judge GREENLIST'S architectural framework as having optimal design characteristics that conform to Fair Information Practice Principles (FIPPS). Such an assessment would fill an important gap in the spectrum of standards for Trusted Identity Attributes. It is with further anticipation that such an action will influence a Federal Reserve Bank's decision to issue an advisory guidance to all banks and credit unions. Such advisory guidance, apart from regulatory mandate, was given for Check 21 when the Federal Reserve Board advised all banks and credit unions to use the NIST standard for Black & White scanning instead of the NIST standard for Gray Scale Scanning.

Licensing and administration of GREENLIST'S root registry and synchronization network can insure that deployment and production operations are instituted consistently, safeguarded permanently, and rendered to be accessible and adoptable by all nations.

THE IMPORTANCE OF TECHNOLOGY STAKEHOLDERS, APART FROM REGISTRARS:
Multi-stakeholder approaches are best even though they can be problematic. How PPI (or some other entity) gets paid for long-term administration of Greenlist source code is the open issue for the governing body of Payment Pathways, Inc. to decide. How questions are asked is important. If the individual doesn't have the skills to respond, what exactly will the authorities' skills be?

This leads to forensics and tools. Those who abuse the Open Source Code of GREENLIST need to be discoverable. Privacy, confidentiality and due process need to be protected.

COMPELLING ECOMOMICS:
New specific purpose for Greenlisting electronic payment addresses is to only receive deposits (and/or requests for explicit permission to debit). These

architecturally imposed restrictions are less risky than dual purpose payment addresses such as the dual automatic debit and credit uses of IBAN as specified by Single European Payment Area (SEPA) or the dual automatic debit and credit uses of the traditional Automated Clearing House (ACH) payment address as specified by NACHA.

In fact, they are much less risky. However there still can be resistance to change in some quarters.

Washington, Brussels, Beijing and Moscow. Is there *any* role at all for some kind of collective governance? Because GREENLIST is concerned about serious business and payments (as well as valuable information asset transfers), the answer is an emphatic YES! But governance without adoption is moot. Only the threat of government sanctioned dis-intermediation of banks by non-bank payment services providers spurs banks to act and adopt.

Markets exist where players are motivated to protect consumers. The Sharing Economy is driving most of the social development on earth. The social net is at the Pong stage of evolution, slowly evolving to the PacMan stage. An administrative framework that synchronizes global GREENLIST registries insures the stability and robustness of the model. The new Identity Attribute is the publicly discoverable electronic payment address. The linkage of this Identity Attribute to Trusted Identity in Cyberspace is the objective of GREENLIST registries. Green means “go” in every traffic signal throughout the world. Applications can proceed, unimpeded, when each registrar’s credentials are known.

The proper role for government is to reflect peoples’ wills. Governments derive their just powers from the consent of the governed. Without sounding pompous about universal inalienable rights, it is gratifying to see NIST/NSTIC advocating for the rights of ordinary human beings.

Thank you for considering our recommendation for a three-way split among banks, governmental agencies and commercial firms. If governmental agencies such as standards and regulators are deemed inappropriate for such a steering committee, then we recommend a 50/50 split between banks and commercial firms for the composition of the governance “steering committee.”