paymentpathways

INTELLIGENT TRANSACTIONS

Greenlist®

PAY IT SAFE

Greenlist®: Protecting Privacy in Electronic Payments

By Richard O'Brien
President, Payment Pathways

Greenlist®: Protecting Privacy in Electronic Payments

Banks can remain the center of their customer's financial lives by providing Positive Pay for eCommerce™, a pathway to universal, ubiquitous, and understandable privacy protection for payments of all types.

As individuals and organizations continue to move from paper payments to electronic for personal and business efficiencies, they also increase the risk of a security breach. If credit card numbers or other regulated payment information is stolen, it can lead to fraudulent transactions and the subsequent need for time consuming steps to monitor, detect, reverse, and resolve unauthorized charges. The examples are many. One of the largest and most recent involved hackers who broke into the customer database at the Sony PlayStation Network in late April 2011. The perpetrators claimed they had access to more than 2.2 million credit cards. Clearly, individuals and organizations require a new layer of security to protect their monetary and informational assets.

Moreover, banks increasingly voice concerns over how to create new sources of non-interest income by growing the volume and value of electronic transaction processing. Recent federal legislation, such as the Durbin Amendment, have spurred banks to prioritize maintaining fee income—or, for the savvy institutions, finding new sources of noninterest income. The breach between banks and their merchant and consumer customers is widening as bank fees become regular media fare. At the same time, the market for emerging mobile payments is massively fragmented, from technology, methodological, and marketing points of view. Clearly, consumers are confused.

Meanwhile, highly publicized privacy breaches, public battles over bank fees, and the continuing cost reasons to make highly personal information, such as medical records, available electronically resulting in federal privacy requirements. The White House has announced the need for more secure, online identifications. "By making online transactions more trustworthy and better protecting privacy, we

Executive Summary

Banks are under increasing pressure from regulators, merchants, and consumers, most notably and recently over debit-card fees. At the same time, payments fraud is an increasing concern and will remain so, especially as person-to-person and mobile payments continue to develop.

So while banks are under pressure to reduce fees, they largely must rely on other providers to tap into those new and potentially lucrative payments markets. The result is decreasing fee income and the transfer of customer loyalty to other payments providers.

The Greenlist provides banks with a common, vendor neutral privacy management solution. It can allow banks to maintain their trusted position as guardians of consumer financial data while generating fee income.

will prevent costly crime, we will give businesses and consumers new confidence, and we will foster growth and untold innovation," President Barack Obama told a meeting with the U.S. Chamber of Commerce on April 15, 2011.

The banking industry will be under increasing pressure. The industry needs to get behind a common standard to protect consumer privacy. In so doing, banks will also protect their central position in the payment system and so enhance bank revenues while meeting regulatory and consumer demands for speed, safety, and accuracy in payments for small businesses and consumers. At the same time, banks need to find ways to send money instantly without sharing revenue with nonbank financial institutions, as many new payment business models require, especially for card-not-present transactions and the rapidly growing person-to-person (P2P) payment markets.

Greenlist provides a pathway for banks to provide privacy protection to consumers while providing instant payment services without revenue sharing. Greenlist allows both parties in a financial transaction to identify each other while keeping secure private data related to the transaction stored with their banks, which can charge for the service. As such, Greenlist can serve as a way to replace fee income lost in regulatory reforms such as the Durbin Amendment while protecting banks' traditional role in the center of the payment system.

With Greenlist, the banks involved in the transaction maintain account information on behalf of their customers without ever needing to release it to another party. Thus each transaction is both instant and completely safe. Banks or third parties responsible for certifying that someone or some entity claiming to be an authorized party is not an impostor can now offer new levels of service at a substantially lower cost for a variety of transactions. Greenlist bank customers can send a payment to anyone, anywhere, and at any time, see the payment posted to the right bank account or debit card immediately, and never

What Is Greenlist®?

Greenlist is a new, patented privacy management system for electronic payments ***only*** available to banks. The system elegantly makes epayments safe and secure without consumers having to disclose any actual account or bankcard information whatsoever.

The Greenlist is also a directory service that verifies identities and payment addresses before transactions are made. It allows payers to locate, validate, and settle the instant transfer of assets. This reduces transfer time and is accomplished without divulging the payee's confidential information.

Banks, the lowest cost risk bearers, maintain the Greenlist by becoming trusted registrars who assume the risk for identity-related fraud based on the information contained within the registry. This transfer of liability substantially reduces the payer-bank's cost of bearing risks because they are left with only those risks associated with payer authentication and authorization—risks entirely in their own control.

need to provide or ask for anything more than a public account name or email address. For consumers, Greenlist is an electronic means to hand a waiter or a florist or a baby sitter a $20 bill; just as fast, just as efficient, and just as secure.

Electronic Payment Promises and Problems

For nearly 40 years banking customers have been able to have their salary deposited directly into their accounts. For more than 20 years customers have been able to set up regular payments to the local gas or electric company, taken electronically from their checking accounts. In 1990 the Internal Revenue Service started encouraging taxpayers to file online, and take refunds by direct deposit. Popularity in this service continues to increase even though many users are charged a fee to file their taxes online. And over the decades of bank website development, bank customers have very comfortable logging on to their accounts and making online payments to credit cards and consumer loans.

But what if your customers want to send money to a child away at college? Pay a babysitter, or the plumber? Or pay an artist in Ireland for a framed photograph that you found on Etsy.com? For modest payments to individuals or small institutions, they often need to write a check, pay cash, or use a debit or credit card. Some major banks have offered online bill payment services, but these tend to require your customer to have access to the bank account number of the party they want to pay. Many smaller vendors (though probably not your baby sitter) offer a payment service, generally PayPal. But most bank customers would much prefer to be able to make payments directly through their own banks instead, and for good reason. PayPal works best when vendors and users both create their own PayPal accounts. In any case, payment recipients must provide PayPal with a lot of personal information to receive a payment, which is not instantly available outside of the monolithic PayPal network. Many customers complain not only about entering this information, but about the excessive spam that results. PayPal restricts their users with a complex set of rules, and requires each party to maintain a balance in a separate online fund that PayPal controls, for making and receiving payments. Finally, PayPal is vulnerable to fraud for those who are not wary.

Recently, however, in response to PayPal, banks and other financial institutions have started offering P2P money transfer services. These offerings have emerged in the last few years to take advantage of improvements in online services and mobile technology, and to offer consumers and small businesses a method for making payments that is faster and more convenient. They have also become popular because they offer an alternative to high fees charged for making payments with credit or debit cards or through existing payment services like PayPal.

At Payment Pathways, we generally do not refer to "P2P," preferring "X2X." In these instant payment transactions, a "person" could just as easily be a small business receiving funds from a person or a small business paying an online merchant.

Payment Service	Description
Chase QuickPay	Marketed as a method that provides low-cost person-to-person wire transfers. A customer can send money to almost anyone with an email address. https://www.chase.com/online/services/quickpay.htm
CashEdge/PopMoney	Marketed to financial institutions as an electronic payment solution that enables consumers to submit payments directly to other consumers (or small businesses) from their personal accounts. Customers can use their online or mobile banking account, and can simply use the recipient's e-mail address, mobile number, or bank account information. http://www.cashedge.com/products-popmoney.php
Fiserve ZashPay	Marketed as a service that allows a consumer to send money to anyone, using only the party's name and email address or mobile number. The money is sent directly from the customer's payment account to the recipient's account. https://www.zashpay.com
Intuit Payment Network	Marketed as a new and affordable way to send and receive payments over the Internet. Designed for individuals and small businesses as an alternative to credit cards and works through QuickBooks. https://paymentnetwork.intuit.com
AMEX "Serve" Payment Network	American Express offers Serve as a fast, simple and secure way to make purchases and to send and receive money to and from friends and family. The sender only needs the recipient's email address. http://www.serve.com
Discover Card-PayPal Money Messenger	Marketed as a free service for sending money to just about anyone using a computer or mobile phone. This method is powered by PayPal and requires the participant to set up a PayPal account. http://www.discovercard.com/sendmoney/?gcmpgn=0311_ZZ_srch_gsan_txt_1

In addition to these services, other companies provide mobile and instant-payment services targeted at consumers and small merchants. Also, PayPal leads the internet-based services and Western Union and others provide traditional alternatives to bank transfers.

X2X money transfers should allow individuals to quickly and easily send small payments to or receive payments from friends, family members, small local contractors or merchants, and charities. Two leading vendor services in this field are PopMoney by CashEdge, and ZashPay by Fiserve. But the reach, so far, is limited. PopMoney was introduced in 2009; as of March 2011

some 200 banks were offering PopMoney to their customers, including CitiBank and PNC. Both vendors plan to offer bank customers the ability to send money directly to and receive payments from Visa-branded credit and debit cards in the U.S. by the end of 2011. By the same deadline, working with MoneyGram, both services look to be able to offer customers the ability to send money to an account outside of the United States. So a bank customer could send $250 safely and directly to his daughter's debit card in another state, or while she is traveling in France. The bank, meanwhile, can reduce processing costs, capture additional fee revenue, and offer an appealing service both to secure the loyalty of existing customers and attract new ones.

But these services are all seriously limited. All share the same flaw, in that none provide a completely secure method for completing transactions. Unlike Greenlist, these competing X2X systems cannot really protect the private financial information belonging to their customers. Each requires the participants to provide their private bank account or bank card information to the other party's payment system to complete the trade. Also, all of these services, even though they are designed to move funds directly to and from the customer's bank accounts online or using mobile devices, work through the automated clearinghouse (ACH). This is the same method used for processing checks; an ecommerce transaction sent through ACH can take several days to complete. This becomes a bigger problem particularly with the psychology related to modern technology. The modern consumer expects instant results with his iPhone or Blackberry when sending messages or checking a GPS map. If electronic payment processing is going to work with mobile devices, they must be instant, too.

The Rise of Mobile Commerce and the Durbin Amendment

Five billion people on planet earth are mobile phone subscribers, including nine out of every ten Americans. In the United States 85% of all pre-teens own a cell phone—73% of them own a book. Apple has sold nearly 60 million iPhones worldwide and Google is activating over 160,000 Android devices a day. In 2009 1.2 billion cell phones were sold. And in 2013, an estimated $30 billion will be spent on phone apps. So besides phone calls and text messages, an iPhone owner can now take a photo of a check and transmit the image to his or her bank, and the amount is added to the owner's checking account balance. Next, mobile device users want to be able to use their phones to pay for groceries or make a contribution to a charity.

The dramatic rise in mobile commerce is forcing banks and merchants and other institutions to find ways for their customers to make payments for person-to-person transactions quickly and easily. We can expect mobile devices to continue to expand dramatically, but the inability of the current services to protect personal information, and the long delay for the transactions to clear,

severely limits the ability—or rather, the willingness—of mobile consumers to move toward P2P transactions. The Greenlist model, addresses all of the issues listed above, solving both of these problems.

Besides new technology, recent regulatory changes also favor X2X electronic transactions. The Dodd-Frank Wall Street Reform and Consumer Protection Act, a sweeping set of reforms to the banking and financial services sector in response to the fall 2008 economic crisis, was signed into law on July 21, 2010. Senator Richard Durbin (D-IL) added an amendment to the bill shortly before it passed that, among many other provisions, places a cap on the fees that banks can charge merchants when customers use debit cards for purchases to no more than 12 cents per purchases. This is nearly 80% less than the current average fee. The political objective was to restrict the ability of debit card issuers to charge excessive fee amounts for the use of these cards, and thus benefit merchants and consumers. Also, as the networks for handling these fees are controlled by just two companies, Visa and MasterCard, consumers and retailers have no choice but to accept these costs of doing business imposed by a monopoly. This regulatory change will cause the fee income banks can charge to customers to drop, and will likely have a dramatic impact on the electronic payments marketplace.

Merchants generally support this reform. The banking lobby, however, has complained bitterly about this rule; they say that the "swipe" fees charged when consumers use their debit and credit cards cover their real costs for these transactions, or are used to provide a subsidy for other services the banks offer their customers. With this limit on fees, banks will need to charge fees elsewhere, such as eliminating free checking and reducing rewards programs. Some smaller banks may need to stop offering debit cards entirely, making them less competitive with larger banks. As of May 2011 the United States Senate was debating whether to delay enforcing the ruling.

But the Durbin Amendment represents an excellent opportunity for the support and growth of X2X instant payment transactions. Privacy management services like Greenlist can provide a way to "recapture" revenue lost through regulatory reforms by increasing transaction volume and value by introducing an instant transfer services for direct person-to-person and person-to-business payments. If a bank customer wants to send money his daughter in college a direct transfer to her checking account or debit card, the debit network can be used if the money needs to arrive instantly. If she can wait for the next banking day, the ACH network can be used, with no swipe fee. Banks that struggle to cover the cost of debit and credit card transactions can offer these two classes of service to merchants and customers and still compete.

Banks, functioning as Greenlist registrars, enroll individuals and small businesses in the Greenlist and assess an initial enrollment fee. A portion of this monthly fee is net income, and a portion of the fee is used as net income for the registry to list debit blocked payment addresses in the public Greenlist. The use of a Greenlist eliminates the potential risk of unauthorized debits by issuing credit push transfers using one of several payment networks, depending on the payment application's requirement.

Coping with Fraud

Many consumers and businesses today are concerned about the growing potential for fraud in electronic financial transactions, and for good reason. According to the International Accounts Payable Professionals (IAPP), by the first quarter of 2011 fraud in electronic transactions had reached $4 billion a year. This represents a steady 1.4% of all sales for the last several years, and an increase from $3.6 billion in fraudulent transactions in 2007. Check fraud is still popular because it is so easy, but according to the 2010 Federal Reserve Payments Study, the number of checks written in the US between 2006 and 2009 fell by over 7%. The number of checks written has been falling for years, and with the rise in mobile payment technology, the decline is likely to accelerate. Future criminals will look for opportunities for stealing money online. Few small businesses can afford to absorb a 1.4% crime tax on their annual revenue, but this level of digital theft is likely to continue unless challenged by improved security technology.

The White House released a national Strategy for Trusted Identities in Cyberspace in June of 2010. The Strategy would promote a national Identity Ecosystem to support trusted online environments. The goal of this Strategy is to develop secure identities that individuals and organizations can apply to virtual commerce that are efficient, easy to use, and applicable across a variety of platforms and systems. These secure identities would allow users to be confident that their security and privacy would be protected while using online services, and would be designed to encourage innovation and personal choice.

The banking sector would likely join in this effort and build a single, secure, global platform to make personal electronic financial transactions fast and easy while protecting the personal information of the parties involved. Merchants and banks also seek to reduce the costs for completing these transactions. The banking industry needs to agree on a uniform standard for making X2X payments and transfers, much like the FIX protocol for trading messages about bank-to-bank financial transactions. Greenlist is a simple and reliable engine for P2P transactions, and could be used as the basis for such a standard. It is capable of using existing technology in the form of current banking networks, like the ATM network, to complete funds transfers instantly. Greenlist

payments avoid the automated clearinghouse with its delays and fees. Further, Payment Pathway's Greenlist service provides an open platform, free of any proprietary network technologies.

How the Greenlist Works

Think of Greenlist as "Positive Pay for e-Commerce™." Just as positive pay services validate checks and ensure that only authorized checks are paid, electronic payments protected by the Greenlist are verified and validated before they are paid.

The Greenlist registry adds another authentication factor that proves that the payer and his device that generated the payment instructions are verified to be authorized. Furthermore, this new factor proves that the account address that receives the e-payment is certifiably owned by the party intended to be paid.

Independent verification of the payer's authorization to pay a correct transaction destination is a "double-check" that does not require any extra user steps or any release of confidential information. In fact, the Greenlist lookup function serves both parties in an X2X transaction to locate and identify each other without either of them needing to release any personal information. With Greenlist, the true account identifiers of both transaction parties never have to leave the banks.

Here's how it works:

Customer Registration

When a person or business registers to use Greenlist, that consumer or business owner provides an easy to remember unique identifier (through a bank portal), often an electronic mail address, mobile phone number or nickname, to serve as their Greenlist ID. These unique ID's are assigned accurate, actionable public payment addresses, which are then stored in a global network of directories managed by Payment Pathways on behalf of its accredited registrars (banks).

These new e-payment addresses are linked to the consumer's primary bank account and/or debit card which the bank or financial institution already has stored on file. The registrar bank also issues the customer a special debit-blocked Personal Account Number (PAN) that conforms to INCITS/ISO/IEC 7812-1-2000 and 7812-2-2000.

The consumer is taught to use this PAN in every card-not-present payment transaction. The bank acts as the custodian for personal and account information in the X2X transaction just as it would for any other financial transaction for that consumer. As a result, the bank retains its trusted position at the center of electronic payments in the consumer's financial life.

Protection for Card-Not-Present Transactions

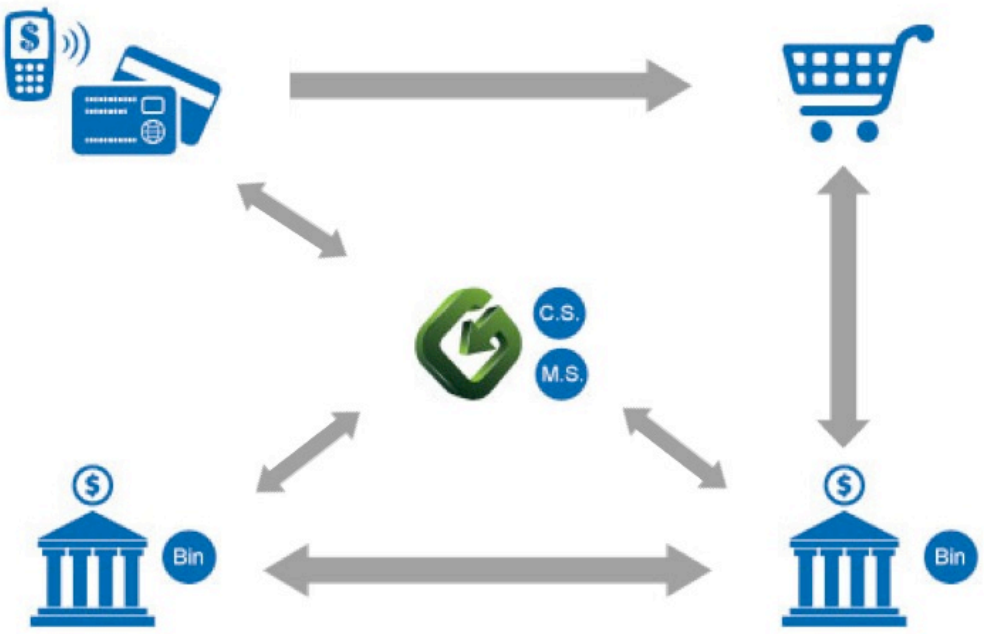
The Greenlist is highly flexible in the kinds of payment transactions it can protect and, as a result, in the number of ways banks can use it to generate income. The following example of a card-not-present transaction between a consumer and an online merchant shows how Greenlist works to protect online payments.

This example features the Greenlist registry, along with servers for matching and communications, to provide both the **Positive Pay for eCommerce** service and authentication factors to mitigate the risks of fraud. The transaction runs on existing payment processing rails with only a few additions to the consumer's device and the merchant's systems.

First, the customer is assumed to be registered with Greenlist through his or her bank, having received a Greenlist ID (GLID) and Personal Account Number (PAN). Also, the **Positive Pay for eCommerce** mobile application has been installed on the consumer's computer or mobile device at the time of enrollment. During that installation, the cloud-based Greenlist application, in concert with the Greenlist mobile app, certifies that the consumer's GLID and Greenlist PAN have been activated.

For their part, merchants, motivated by their desire to reduce fraud losses from systemic chargebacks, have added a few lines of code (Greenlist libraries) in the checkout part of their shopping carts to support Greenlist interactions and to provide **Positive Pay for eCommerce**.

For Greenlist registered consumers and merchants, here's how a card-not-present transactions with Positive ePayment works:



1. The Consumer (Payer) uses his or her computer or mobile device to initiate making a payment via the online Merchant's web portal. The consumer's Greenlist PAN (essentially, a Greenlisted Debit Card Number) will be used as the chosen payment method.

2. Code in the Merchant's system queries the Greenlist (or special bin lookup) to find out whether the customer's card number is a valid Greenlisted PAN. If the response is positive, it returns a simple positive acknowledgement including the consumer's phone number. Then the Merchant's system:
   - Queries the consumer's Greenlist app for its Greenlist ID by sending a Greenlist Query Message in a prescribed format that includes the Merchant's GLID via SMS. The mobile device generates an automatic response used to validate mobile device as the source of the Greenlisted PAN given to the merchant.
   - Sends transaction initiation information, including the Greenlisted PAN, to the Matching Server (MS). There the information is date-time stamped, hashed, and stored.
   - Processes the payment request to the Consumer's bank through its usual payment processing network.

3. Note that if there is no valid response from the Greenlist mobile app, the Merchant will continue processing the payment request as usual. However, the Merchant would not ship product without a confirming message from the consumer's bank; lack of a response means that the probability is high that the payment will not be explicitly authorized by the true card holder.

4. The matching server (MS) verifies the PAN received from the Merchant and waits to correlate it with a corresponding transaction verification request from the consumer's bank. The matching server can be either owned by the bank and kept on the premises or accessed through the cloud, depending on bank preference. Note that the matching server only receives the consumer's PAN if the Merchant was successful in querying the Greenlist app installed on the consumer's mobile device (or PC). By previous agreement with the merchant, card issuing bank, and acquiring bank, the Matching Server will have up to 60 minutes to receive and process a matching transaction verification request from the consumer's bank. If none is received during that time, then the card issuing bank will reverse the payment authorization.

5. The consumer's bank processes the payment request from the Merchant's system. It verifies that the PAN is not in the bad-number bin, and finds the PAN in the Greenlisted bin. Having

verified the PAN, the consumer's bank makes sure that the consumer's actual bank account has sufficient funds available to cover the purchase. If funds are available, the payment authorization is sent to the merchant in the usual manner.

6. Because the consumer's PAN was found by the card issuing bank to be in the Greenlist bin, a **Positive Pay for eCommerce** check is now initiated. The card issuing bank sends the transaction information, including the consumer's PAN, the Merchant's PAN, and the payment amount, to the Matching Server. The Matching Server time stamps, hashes, and stores this information upon receipt. Then the Matching Server searches for earlier transaction information that would match the information just received.

7. If the Matching Server discovers a valid match, i.e., if the debit received from the merchant matches the transaction information provided by the consumer through the Positive Pay for eCommerce application within the 60 minute window, then the bank maintains its 'Payment Authorized' message that was previously delivered to the merchant. The transaction is settled through the existing payment network infrastructure to the merchant's bank, and a credit is posted to the merchant's account in the usual manner. If the Matching Server does not discover that a previous transaction had been submitted within the past 60 minutes, the Matching Server will decode the merchant name by doing a reverse lookup of the merchant PAN in the Greenlist registry. Then:
   - The Matching Server passes on the amount and merchant name with the consumer's contact information to a Callback Server. These values are found with a reverse lookup to the Greenlist registry using the consumer's PAN.
   - The Callback Server (CS) contacts the consumer's mobile phone associated with the consumer's Greenlisted PAN to inform the consumer that the payment was not verified. It asks the consumer to verify or cancel the transaction. The message can be sent as an automatic telephone call, a text message, or an email message, depending on what the user's preferences obtained during enrollment.

8. If the Matching Service determines that the transactions do not match, then the consumer's bank notifies the consumer to obtain his or her authorization through a pre-arranged channel, such as a phone call or text message. If the payer does not authorize the transaction, then the transaction is reversed through the merchant's bank.

The major benefit of the Greenlist, again, is that no personal or sensitive information (beyond what merchants require for shipment of physical goods or licensing digital goods and services) had to be provided. The card issuing bank enforces that the consumer's PAN can never be used to generate an automatic debit without a Positive Pay authorization, proving that the consumer's PAN indeed was input from a smart phone or PC device containing an installed app with a properly enrolled GLID.

If a fraudster uses a stolen Greenlist PAN to pay for a subscription or recurring bill payment service, the consumer is protected by the mobile apps' logic that would either discover a.) that merchant's PAN is not in the Greenlist at all and NOT respond affirmatively to the merchant query or b.) the merchant is legitimate but a stolen PAN is paying for someone else's benefit.

In the second case, the merchant's query to the mobile app would fail because the merchant's GLID would not be in the app's approved list of payee GLIDs for subscriptions and recurring billpayments. In this scenario, the legitimate merchant does not submit the PAN, the match then fails and the consumer would be notified. If the consumer input his Greenlisted PAN into a subscription service from his PC but forgot to add the Merchant's GLID to his mobile app, it would be automatically added for him when he is called back the first time for that merchant by his bank's Positive Pay for eCommerce service.

Hackers would never have money sent to a Greenlisted PAN because that would paint a clear trail to their doorstep.

This Positive Pay for eCommerce service is feasible and straightforward for all parties because the transaction mechanisms and procedures for high-volume uses like card-not-present transactions are well understood. Capital expenditure required of the bank is minimal.

Future Content Transfer Applications

Greenlist doesn't just protect users from fraud. Personal information can be used—and misused—in other ways. Indeed, the most contentions battles in ecommerce involve not the transfer of payments but the transfer of content, including music, movies, and news. Moreover, the future growth of electronic transactions involves highly sensitive informational assets, including securities, medical records, insurance and education information. To this end, Payment Pathways has recently received a second patent that facilitates the transfer of such non-monetary assets under supervision and control of various communities of interest leveraging the same privacy protection and authentication as the Greenlist provides banks to remain central in electronic transfer of funds.

This is the subject of a future whitepaper.

Conclusion

Consumers, banks, merchants, and charities would eagerly adopt an electronic payment system that really works. A variety of new solutions have been introduced in recent months, but for any one of these electronic payment services to thrive, it must become as ubiquitous as the mobile devices that would be used to access them. Yet with the currently developing services, consumers and businesses must reveal private financial information. This has long been a source of resistance to electronic payments systems. Further, all competing payment services send their payments through the Automated Clearing House, taking three business days for the payments to post.

Payments using the Greenlist service are credited and debited instantly using existing electronic payments networks. The economy would support a much faster move from payment systems using cash and checks to personal electronic funds transfers, so that, with an iPhone, Charlie can send his friend Rick money for play tickets, or Tom can pay for dinner, or a garden center can pay a vendor for a delivery of flower seedlings. But before this can happen the financial sector needs to provide a means to identify both parties in a transaction without requiring either one to reveal any private information, and complete the transaction in three seconds, rather than three or four days.

Greenlist can meet that need. Greenlist's open architecture enables search and retrieval of trusted identity information related to electronic payment transactions. This service can work with any existing payment system or network.. Individual consumers can trust their bank's Greenlist to manage transactions promptly while protecting their private information. Each bank can charge a fee to query of one of several Greenlisted identifiers to find a Greenlisted payment address to be used by the payers' bank to originate a payment.

In the end, all payment network stakeholders benefit. The volume of credit payments and income increases without new capital expenditures. The thin nature of the directory and its search function adds a new factor of authentication to safeguard bank payment transactions without adding the burdens of regulatory compliance or paying for additional technology. At the same time, banks remain at the center of the payment process, generating revenue from registrations and transactions.

About Payment Pathways

Payment Pathways, Inc. (PPI) provides patented privacy management software and payments identity solutions. Our Greenlist® elegantly makes epayments safe and secure without requiring disclosure of any actual account or bankcard information whatsoever. PPI also offers consulting

services. We help all parties in the payments ecosystem with payments privacy, service profitability, and identity protection.

Payment Pathways has received two patents for its technology.

The company's management team has worked in the electronic banking, payments, and network industries since the late 1970s. PPI also currently has three investment partners with extensive experience in identity management services, banking, and electronic payments:

- Dollar Bank F.S.B. of Pittsburgh, Pennsylvania
- Authentify, Inc. of Rosemont, Illinois
- Zenith Information Systems, Inc. of Los Angeles, California

Richard O'Brien // President and CEO
Payment Pathways, Inc. // 200 S. Wacker Drive // 15th Floor // Chicago // IL 60606
Office: 312-346-9400 // Facsimile: 312-276-8810 // Mobile: 630-715-0956 // Email: robrien@paymentpathways.com

