



A Safe and Easy Way
to Make Fast Electronic Payments

By Richard O'Brien
President, Payment Pathways, Inc.

You are used to having direct deposit only for your paycheck; you probably have your monthly utility bills deducted from your checking account automatically each month. Rather than sending a check to Visa or MasterCard, you simply pay your credit card bills from your bank's web page. The same goes for your car payment. You make the IRS happy by filing your 1040 form electronically each year, and they in turn make you happy with an electronic deposit of your refund directly into your checking account a week or two later.

Electronic payments are nothing new. But by the early 21st century they should work much better. You can pay off your credit card balance online, but what if you want to send \$100 to your sister in Ohio to help pay for a family party, and she needs the cash now, not by check next week? What if you want to pay a babysitter, or the kid who mows your lawn for you twice a month? Suppose you only have \$2 in your wallet, but you're at the farmer's market and you want to pay a produce vendor \$25 for organic vegetables and cut flowers? What if you enjoy a band playing at that same market, and you want to give them \$10 for a CD and a contribution?

For bankcard transactions, we live in the era of the Internet. But for simple cash transactions, we return to the days of Queen Victoria and Rule Britannica. Write a check, put it in the mail. Pull out cash. Why can't we use technology to make simple financial transactions quickly and easily in 2011, and without being afraid that we will get ripped off?

Waves of companies offer online bill aggregation and payment services, but these require that you provide your bank account number and require billers to register which is not ideal for spontaneous bill presentment and payment. Many smaller vendors (though probably not your baby sitter) do accept PayPal. Many prefer to be able to make payments directly through their own bank instead.

PayPal and the New EPayment Systems

To use PayPal effectively you need to set up an online account, and to do that you need to provide them with your bank account or bankcard number. Withdrawing money, like cashing a check, takes several days to process. You may receive a lot of spam as a result and you may not like PayPal's complex set of rules such as the requirement that you maintain a balance in a separate online fund that PayPal controls before you can send and receive payments. Finally, making transactions via PayPal is a great way to get burned by an online thief if you aren't careful to regularly monitor your bank account or bankcard statements.

Recently, however, in response to PayPal, Western Union and the like, banks and other financial institutions have started offering Person-to-Person (P2P) money transfer services that work with either a personal computer or a mobile device. These services have emerged in the last few years to take advantage of improvements in online and mobile technology and to offer consumers a payment method

that simply requires they know the recipient's email or cell phone number. They also offer an alternative to high fees charged for making payments with credit or debit cards or through existing payment services like PayPal. ClearXchange, the P2P system offered by Chase, Bank of America and Wells Fargo, legitimized this space — covering 49% of all bank accounts in the U.S. Within weeks of the public launch of ClearXchange, Fiserv and CashEdge announced they are merging their respective P2P and B2B payments systems to form a common network to accelerate market adoption and usage. Their research indicates that most people prefer to perform their own account transactions at their financial institution. This consolidation effort clearly shows that P2P services offer significant opportunity for FIs today, and should grow in the future. For instance, CashEdge banks report that the pace of enrollments surpasses the pace of enrollment in their original online bill-payment service enrollment.

But will growth be optimized for banks and consumers alike? ClearXchange and Fiserv (Fiserv is acquiring CashEdge pending regulator approval) operate separate registries behind secure and encrypted bank firewalls. Both services require off-net receivers to divulge their bank account numbers in order to receive a payment. This only works if one really trusts an email from a different bank asking for confidential information in order to get paid. Many people are savvy to phishing, pharming and Nigerian scams.

*Financial institutions that have deployed CashEdge's Popmoney for at least a year report 6% to 8% penetration of their online banking customers.¹ Could the reason be that just a small percentage of people were expecting to receive a payment and therefore were willing to risk putting their true bank account 'out there' via the Internet? Wouldn't it be safer to have a payment address that can only **receive** deposits? One that's safe to reside in a public registry? One that's linked to easy-to-remember unique identifiers? CashEdge reports that their bank customers indicate that the pace of PopMoney adoption surpasses the pace of early on-line bill payment adoption.*

These money transfer services should allow individuals to quickly and easily send or receive small payments with friends, family members, small local contractors or merchants, and charities. But they all share the same flaw: none provide a completely secure method for completing transactions. They cannot really protect your private financial information from falling into the wrong hands. Each one requires the recipient to provide his private bank account or bankcard information to the other party's payment system. Few trust email messages asking for their bank account number.

If you do trust the message and **are** expecting a payment, many of these services move funds through the electronic payments network known as the ACH, which serves as an electronic substitute for checks. It's the system that processes your direct deposit, the direct debits of utility, and other bills from

¹ March, 2011, Issue 968 The Nilson Report

your checking account. It's efficient, inexpensive, and secure enough for regular recurring bill-pay, if one takes the time to divulge their bank account to trusted billers.

But it also takes **two to three days** before funds are credited to an account and are made available to spend. So, just like writing a check, your ecommerce transaction sent through ACH can take several days to complete. That leaves us back where we started—you are texting with your iPhone or checking a GPS map while riding horseback next to your family's covered wagon along the Oregon Trail. You get emails promptly; why can't payments you receive with your mobile device be processed instantly too?

The Fair Information Practice Principles (FIPPs) are the widely accepted framework for evaluating and mitigating privacy impacts. The eight FIPPs are transparency, individual participation, purpose specification, **data minimization**, use limitation, data quality and integrity, security, and accountability and auditing. To eliminate one's risk of financial fraud, the Data Minimization and Use Limitation Principles should be observed when creating the identity attributes for a publicly discoverable electronic payment address. The National Strategy for Trusted Identity in Cyberspace managed by the National Institute of Standards (NIST) agency of the US Dept. of Commerce is soliciting input from industry for governance recommendations for registry & use of various aspects of identity in this electronic age.

Greenlisting: The Secure, Public Alternative

Payment Pathways offers banks a simple, safe, and easy-to-use solution: Greenlist®. In essence, Greenlist is a synchronized network of public directories of personal electronic payment addresses. It is a 'hiding data' technology. Its invention is described in its U.S. utility patent for a privacy management system for electronic payment addresses. The system insures that your registered epayment addresses can only receive funds and are publicly discoverable so payments can be made to you that are safe and secure. You never again have to tell anyone, any merchant or any payment system your actual bank account or debit card number.

Greenlist acts as a trusted registry of public payment addresses that every party in a transaction can access and use to identify each other. So when you want to send a payment or a request for payment to a friend or relative, a business, or an institution, Greenlist validates the party on the other end of the deal.

Your Greenlist address can be anything that you can remember easily and don't mind sharing with others, such as your email address or cell phone number, as long as it's unique. Your bank maintains all of your private account information for you, just as they do now. The banks that send or receive funds on your behalf, and the banks issuing debit cards, never need to reveal your actual account number or other sensitive information to anyone else.

What Greenlisting Provides

Greenlisting reduces a bank's risk of processing instant online payments by listing public payment addresses for discovery by its payers. It protects the private payment identities and bank affiliations of consumers by providing public payment addresses for deposit-only bank accounts. Consumers' real bank account numbers never have to be given to merchants or payment processor networks. The US FRB's FedGlobal office reports that in Costa Rica, where banks routinely use a registry of electronic payment addresses, the annual number of returns reported for unauthorized debits have been reduced to zero!

This method can even provide an extra layer of security in that your bank can confirm every payment before it settles. GreenlistIDs can be used to instantly compare your payment records from a registered device like a smartphone to a merchant's payment request. If they don't match you will receive an automatic phone call or message asking you to confirm the payment. This fraud mitigation countermeasure engages consumers in a new and meaningful way for card-not-present transactions and it is eligible for additional bank compensation under rules in compliance with the Durbin Amendment to the Dodd-Frank Financial Reform Act. More importantly, **Positive Pay for eCommerce™** counters the technical sophistication of cybercriminals which is swamping the world's ability to cope.

To use Greenlist your bank or payment service provider does not necessarily have to offer Greenlist. Only the people or businesses you want to receive payments need to sign up for Greenlist. Some banks may charge a fee to register for Greenlist; after that most banks using Greenlist will charge a fee to senders of instant transactions. Faster and more convenient, fees would be competitive with Western Union payments. Next day payments would cost less and in many cases, be free. For other payments fees are charged to the merchant. Fees for maintaining and using the Greenlist are born by merchants who benefit by prevention of fraud and systemic chargebacks.

Greenlist works out for everyone. You can protect your sensitive account information by using a universal, public, and secure payment address. Online merchants can send goods knowing that the person who paid is actually the person who placed the order. Banks take on reduced risk of payments fraud and earn new income two ways: from the increase in payment volume and the higher value of instant payment services. Ultimately, society as a whole also benefits because Greenlist can provide a way for people who do not now have banks accounts or under utilize them to become part of the electronic payments system in a low-cost, secure way.



Richard O'Brien
President and CEO

Payment Pathways, Inc.
200 S. Wacker Drive, 15th Floor
Chicago, IL 60606

(312) 346-9400
(630) 715-0956
Email: robrien@paymentpathways.com