February 22nd, 2011

Nandan Sheth
President and COO

Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th St. and Constitution Ave.
NW Washington, DC 20551

Dear Ms. Johnson:

On behalf of Acculynk, LLC, the U.S. provider of PIN-debit payments online, we are grateful for this opportunity to provide comments on the Proposed Rulemakings for implementation of the Dodd-Frank Act mandates for debit cards. And we commend the Fed team for its considerable effort and skill in attempting to help restructure a business that can clearly use more competition and innovation.

The technology for encrypting PINs with software has been in the marketplace for more than decade with predecessor companies; since acquiring this technology in 2008, Acculynk has leveraged this experience into a quickly-growing alternative to signature-debit for purchases over the Internet. We believe this decade of experience affords us an unusual and valuable perspective that the Fed might not have been exposed to before.

In particular, we believe that the PIN-debit online solution described in our "Comments" submission, and explained in detail in our "Rationale for PIN-debit Online" white paper and its accompanying documentation, actually offer constructive, readily implementable solutions for online debit card use that satisfies the spirit and intent of the four Rulemakings. Contrary to some submissions in the initial round of commentary, PIN-debit works very well online, and can work equally well for mobile payments. As such, it helps round out the case for enabling PIN-debit to emerge as a preferred embodiment for removing fraud from the payment system in every transactional venue.

Specific Requests for Comments from Proposed Rulemakings

Interchange Rate Alternatives

The principal perspective we can offer is that use of PIN-debit online can dramatically reduce transactional fraud, charge-back costs and customer service activities—to the extent that use of PIN-

debit online facilitates growth in new transaction volume and, over time, replaces signature-debit card use. This will enable issuers to have a better opportunity to reduce their debit card costs, and a better chance at making a profit—within the recommended cap on rates.

Fraud Adjustment

The Board requests comment on how to implement an adjustment to interchange fees for fraud-prevention costs. In particular, the Board is interested in commenters' input on the following questions:

1. Should the Board adopt technology-specific standards or non-prescriptive standards that an issuer must meet in order to be eligible to receive an adjustment to its interchange fee? What are the benefits and drawbacks of each approach? Are there other approaches to establishing the adjustment standards that the Board should consider?

In the case of online debit card use, there are three options that could be considered:

a) technology-specific standards;

b) non-prescriptive standards;

c) industry mandated standards.

Each option differs with regard to the likelihood and timing of market adoption as well as the consistency of security benefits offered. These variations are quite different for online debit usage in several important ways.

a. Technology specific standards
Technology-specific standards offer strong guidance, without an actual mandate, for what forms of PIN-debit protection will be effective online, and therefore fairly compensated.
For online use, PINs can be included in the debit card transaction with three forms of protection:

i PIN-equivalent substitutes
ii. Hardware-encryption;
iii. Software-encryption;

i. The first option, PIN-equivalent or substitute alternatives cannot be viewed as sufficiently secure, and have not experienced consumer adoption. For example, one-time passwords, or pseudo-numbers, have been tried extensively over the past five years, but largely abandoned. The major hurdles were the tasks consumers had to perform to use them, and the difficulty using them in real-time and unfamiliarity of resolution when problems arose. Also they did not provide the consumer and merchant protections that true PIN-debit does.

The other two options--hardware and software encryption—utilize the PIN, and the EFT networks,

directly; they have much more relevance as a sustainable solution for eCommerce, as discussed further in the accompanying white paper.

ii. Hardware-encrypting devices plugged into cardholder Internet devices can certainly perform the security required, but have several drawbacks such as cost of the devices, user difficulties with installation, aversion of users to additional equipment, potential operational issues, etc..

iii. Software-encryption methods are now every bit as secure, and when presented as a host-served PIN-input screen (e.g., with a floating PIN-pad interface that mimics the user ATM experience), require minimal change in behavior or deployment cost for issuers or consumers, and very modest costs for online merchants. Some investments are required by the EFT networks, but those are not considered to be substantial, and would be incurred in any deployment of online PIN verification for authorization.

Thus, a technology-specific standard that weighed the interests and investment/deployment requirements of all parties, *and* narrowed the choice of technology (e.g., software-encryption) at a sufficient standard of security (e.g.Triple-Data Encryption Standard,128 bit keys, as required for ATM and EFTPOS transactions) would suffice for providing a particular design configuration to the marketplace that would still allow substantial variations in actual deployment options—in this case, the application of the software encryption algorithm.

b. Non-prescriptive standards

Allowing the marketplace to deploy PIN-debit online with non-prescriptive standards (e.g., any mechanism that performs 128-bit triple-DES conversion of the entered PIN at inception all the way through to the EFT network) would most likely perpetuate the extensive and mostly unproductive experimentation with deployment options and variations, without consistency in monitoring and auditing the security.

c. Industry mandated standards

The third option—an industry mandate (such as requiring *every* EFT network to offer software-encryption online PIN-debit within a certain time period, and perhaps a prescribed user interface for PIN-entry)—has the benefit of rationalizing total industry investment around a preferred solution that has consistent security and user interfaces and minimizes merchant confusion and acceptance costs. Clearly, this perhaps more determined posture might be viewed as running counter to the Fed's traditional restraint from endorsing specific solutions, but in the aftermath of the banking crisis, and in a post-Durbin environment, the need to minimize investment costs (and forestall continuing fraud losses) should be factored into its consideration.

Any such consideration should be viewed as transitional, rather than permanent, in any event. The progress of technology is relentless, and any industry standards developed and promulgated for the U.S. market should eventually flow into international standards ,e.g., ISO 20022, which has as an initial

thrust standards for common debit card usage across borders. That will ensure new solutions that offer better protection and performance make their way into the payments marketplace.

2. If the Board adopts technology-specific standards, what technology or technologies should be required? What types of debit-card fraud would each technology be effective at substantially reducing? How should the Board assess the likely effectiveness of each fraud-prevention technology and its cost effectiveness? How could the standards be developed to encourage innovation in future technologies that are not specifically mentioned?

The preferred deployment—based on a decade of experience—for PIN-debit online is a technology that has the following principal components:

- 1) Protection of the PIN (and PAN) throughout entry and submission process via a secure host;
- 2) A natural, logical and secure user interface for PIN-entry;
- 3) Efficient merchant access to as many EFT networks and debit card accounts as possible;
- 4) Integration to as many EFT networks as possible from the secure hos
- 5) All provided in software that is easy to install and updatable across the system.

Once deployed, such technology will address both unfriendly and friendly fraud across-the-board, and will lead to substantial decreases in risk management and fraud reduction investments as the use of signature debit, card not present transactions declines over time.

The Fed can examine the relative risks and fraud reduction experience of PIN versus signature debit cards at the POS historically, and apply the same experience to online and mobile transaction venues. Metrics for both are now available, or can be obtained from either cooperating merchants (signature-debit versus signature-credit typically is only know by processors, and/or issuers, and they can be monitored over time and by merchant vertical.)

The Fed can also be instrumental in evaluating the preferred deployment with encryption algorithms, communications security, etc., then input these to trigger consideration and adoption by the various standards bodies in much the same way it does today. PIN-debit, which is based on the common and near-universal ISO 8583 format and its associated standards (and already is heavily examined and vetted for its 128-bit triple-DES for use at ATMs and via POS terminals) should translate easily to existing Internet standards and emerging mobile standards.

3. If the Board adopts non-prescriptive standards, how should they be set? What type of framework should be used to determine whether a fraud-prevention activity of an issuer is effective at reducing fraud and is cost-effective? Should the fraud-prevention activities that would be subject to reimbursement in the adjustment include activities that are not specific to debit-card transactions (or to card transactions more broadly)? For example, should know-your-customer due diligence performed at account opening be subject to reimbursement under the adjustment? If so, why? Are there industry-standard definitions for the types of fraud-prevention and data-security activities that

could be reimbursed through the adjustment? How should the standard differ for signature- and PIN-based debit card programs?

Non-prescriptive standards for PIN-debit online would likely include hardware-encryption, software-encryption, and PIN-equivalent alternatives—fashioned to perform largely identical functions, but likely with extensive variations in security. So the task of setting non-prescriptive standards would be difficult to derive, and it would not be certain how well they would work and scale, given the lack of high-volume/high-exposure experience.

Since issuers do relatively little in the way of online fraud management, and that is limited to signature-based cards, and further, that activity is more often than not outsourced to processors, where there is little differentiation between signature-debit and signature-credit, it is not clear that any fraud 'offset' makes sense for continued use of signature-debit.

PIN-debit online, as implemented by Acculynk, imposes no requirements on issuers, including no extra security requirements, but its adoption provides incremental benefit to the quest for fraud reduction overall for all. As an incentive for adoption, issuers should collect a fraud reduction 'offset' for deploying PIN-debit online. The mechanism in place of charging to merchants a merchant service fee that is comprised of interchange and acquirer mark-up provides a platform for enabling this value exchange between issuers and merchants

It does make sense to develop industry standards for debit card going forward, and there will be substantial differences for signature-debit versus PIN-debit. Given an even playing field for deployment, PIN-debit could be expected to continue to produce far less fraud than signature-debit, and has the added virtue that it can be instrumental in reducing so-called 'friendly fraud'. Industry estimates put the friendly fraud rate (where cardholders repudiate transactions that they actually know about but claim to be fraudulent and unauthorized) at 30-50% of today's online transactions. Similarly, a significant portion of online charge-backs occur for extraneous, and fraudulent, claims of non-receipt/non-delivery; issuer innovations in helping merchants eliminate this type of fraud would be welcome, too. Most importantly, issuer initiatives in reducing the number of charge-back 'recidivists'—across both signature-based and PIN-debit payments, in both online and offline venues—would be innovations worth rewarding.

4. Should the Board consider adopting an adjustment for fraud-prevention costs for only PIN-based debit card transactions, but not signature-based debit card transactions, at least for an initial adjustment, particularly given the lower incidence of fraud and lower chargeback rate for PIN-debit transactions? To what extent would an adjustment applied to only PIN-based debit card transactions (1) satisfy the criteria set forth in the statute for establishing issuer fraud-prevention standards, and (2) give appropriate weight to the factors for consideration set forth in the statute?

In general, the Fed should emphasize adoption and use of PIN-debit—online and offline and in any other venue—because of its superior consumer preference and performance, vis-à-vis signature-debit. Use of PIN-debit online means shifting the bulk of risk management and fraud prevention to the issuers, so if

issuers are able to improve upon the inherent ability of this payment type to be more secure, they should be compensated for it.

5. Should the adjustment include only the costs of fraud-prevention activities that benefit merchants by, for example, reducing fraud losses that would be eligible for chargeback to the merchants? If not, why should merchants bear the cost of activities that do not directly benefit them? If the adjustment were limited in this manner, is there a risk that networks would change their rules to make more types of fraudulent transactions subject to chargeback?

Merchants should only pay for value they receive; if issuers' adoption of Internet PIN Debit leads to fraud mitigation and chargeback improvements , that is a great benefit to merchants and issuers. With respect to network rules governing treatment of fraud and classification of charge-backs, it is logical that guidelines be established and managed in a manner that prevents manipulation that results in any particular party being disadvantaged vis-à-vis the other party (e.g., policies that might encourage 'friendly fraud'). One possible manifestation of this new philosophy is to eliminate the Card Not Present (CNP) distinction that has characterized eCommerce for the past decade, and acknowledge that secure PIN entry and verification enable card use that is at least as strong as Card Present at POS (and in some respects offers stronger security).

6. To what extent, if at all, would issuers scale back their fraud-prevention and data-security activities if the cost of those activities were not reimbursed through an adjustment to the interchange fee?

Issuers should offer and support payment products that are secure and efficient; signature-debit clearly does not meet that criterion. However, if issuers are willing to take proactive steps, for the benefit of all stakeholders in the payment value chain, and invest in incremental fraud mitigation , a fraud adjustment makes good sense.

For example, part of implementing Chip+PIN is making the PIN available for every transaction in every venue; so while a fraud reduction 'offset' for implementing PIN-debit online is a logical inducement for issuers to deploy it, if such an incentive were not available, most issuers could be expected to still be motivated to deploy it for the 'good of the system', and to avoid operating at a cost disadvantage versus competitors.

A similar logic should work for merchants—even without some sort of financial inducement to adopt PIN-debit (or interchange 'surcharges' for delaying investment in Chip+PIN components, as occurs in some EMV deploying countries), merchants could be expected to deploy at least the PIN-entry and authentication component, since it would reduce their costs for debit card processing.

7. How should allowable costs that would be recovered through an adjustment be measured? Do covered issuers' cost accounting systems track costs at a sufficiently detailed level to determine the costs associated with individual fraud-prevention or data-security activities? How would the Board determine the allowable costs for prospective investments in major new technologies?

Issuer DDA systems tend to operate at a generic level for dozens of functions and modes of access, and usually combine fixed, semi-fixed and marginal costs together, spreading them across the entire line-of-business. This makes accounting for actual, incremental costs—as seen in the September Fed survey results—very difficult to measure. Guidance from the Fed (and other regulators) on how to improve the cost accounting for debit cards (and other banking products) would be enormously helpful for moving the industry to a more meaningful representation of their revenue, costs and profitability. Until that time, the Fed should avoid simply rebating or refunding part or all of issuer investments, and such investments should utilize new, standard metrics for returns on those investments. Thus, a holistic fraud mitigation and risk management 'system' needs to be created (perhaps embracing some of the best-practice accounting conventions of the most advanced banks and credit unions).

Such advances in accounting can and should be embraced by the core system provider outsourcers for most of the nation's smaller banks and credit unions—avoiding incremental costs of upgrading individual general ledger systems for more than 16,000 financial institutions. Perhaps a task force of industry accountants, consultants, auditors, core systems providers and other experts could be created and charged with doing this needed work. Such initiatives, for the 'good of the system' could easily be funded by temporary 'click' charges on transactions, collected from the merchants and allocated back to the issuers.

8. Should the Board adopt the same implementation approach for the adjustment that it adopts for the interchange fee standard, that is, either (1) an issuer-specific adjustment, with a safe harbor and cap, or (2) a cap?

9. How frequently should the Board review and update, if necessary, the adjustment standards?

A thorough assessment and benchmarking (which the Fed has begun with the surveys in September) conducted for a finite period of time (say, three years) would go a long way to providing a baseline for gauging industry performance. After this period, an annual audit would provide a basis for reviewing the effectiveness of industry's efforts against the always-growing

10. EFTA Section 920 requires that, in setting the adjustment for fraud-prevention costs and the standards that an issuer must meet to be eligible to receive the adjustment, the Board should consider the fraud-prevention and data-security costs of each party to the transaction and the cost of fraudulent transactions absorbed by each party to the transaction.

How should the Board factor these considerations into its rule? How can the Board effectively measure fraud-prevention and data-security costs of the 8 million merchants that accept debit cards in the United States?

Some of those 8 million merchants are clearly online (and more than million merchants are web-only). There, the great preponderance of fraud losses and risk management costs are borne by the merchants (76% according to the September survey). Ideally, banks, which have great knowledge about account use, behavior, and cardholder identity, should be incented to work with merchants, which have great

knowledge about what happens in a transaction session. Unfortunately, the rules of Card Not Present (CNP) relegate the liability and responsibility to the merchants, and issuers effectively do not exert much effort and investment toward reducing risk at their end.

So, effective measurements would need to define what the issuer contributes to the process. Issuers might be incented to deploy and record results, and then begin to assemble best practices. In particular, it would be very valuable to incent and embrace efforts to work with merchant data to derive a more holistic risk management paradigm for both online and mobile transacting. If, as expected, PIN-debit performs substantially better than signature-debit, it might be constructive to encourage the industry to quit investing in trying to protect signature-debit, and channel its efforts and investment to ensuring that PIN-debit remains the safest payment system in any venue.

Network Exclusivity/Competition

A hosted system for PIN-debit online is purposely designed to interconnect with all EFT networks and all of their members and accounts; so creating a standard for PIN-debit use for Internet (and mobile) transactions naturally fosters a full selection of networks for consumers and merchants to choose from. In order for network competition to be able to play out, debit cards need to carry at least one network that supports Internet PIN Debit. Otherwise, transactions will default to the signature network of record.

<$10 billion exemption

The complexities of ensuring all smaller financial institutions can participate at POS on an equal footing with banks and credit unions with greater than $10 billion in assets does not exist online for PIN-debit online. The host-system configuration (please see accompanying description), when connected to as many EFT networks (and cardholder accounts) as possible, provides a level playing field that lets the EFT network solution at the merchant website drive the transaction authorization and settlement to the card issuer—rather than being redirected by the merchant to some other issuer with perhaps a lower interchange. As well, the pricing model (used by Acculynk to-date) sets the price at a standard rate from the networks and the permitted rate by issuers, along with a negotiated rate from the merchants (which includes tiered pricing based on overall volume). Therefore, the structure for PIN-debit online has no mechanism for price discrimination, but can accommodate whatever the networks decide to charge—including proposals such as Visa's to support a bifurcated rate. Such pricing neutrality would not exist for signature-debit.

In conclusion, we believe that Acculynk offers constructive, readily implementable solutions for online debit card use that satisfies the spirit and intent of the four Rulemakings. In the white paper provided under separate cover we have provided further background and details about this solution.

In closing, we appreciate the Board's consideration of the view we present in this white paper on the proposed rules around debit card interchange. We would welcome the opportunity to schedule a personal meeting to discuss the points presented in this paper more fully.

Sincerely,

Nandan Sheth

President and COO, Acculynk, Inc.

Submitted February 22nd, 2011

"Rationale for Internet PIN Debit"

Submission to the Federal Reserve Board

From Acculynk, LLC

Delivered February 22nd, 2011

Table of Contents

Acculynk is a privately-held, venture capital funded company based in Atlanta, GA, which has made significant investments in developing intellectual property and developing the market for the use of ATM debit cards with PINs in the U.S. Currently nine of top twelve EFT networks in the U.S., have certified Acculynk's core product, PaySecure, for use. The product resides on a secure host system that serves online shoppers with a PIN-entry window on their PCs or mobile devices when they select PIN Debit for payment on accepting merchant websites. The PIN-entry process is secured by a 'floating PINpad' graphical convention that prevents detection of the numbers being entered. Additional background information on the company is provided in Appendix A.

1. Executive Summary

Collective research and experience have demonstrated that PIN Debit transacting is the most popular way to make payments for consumers and merchants alike, as well as providing a better solution for the banking industry than signature debit. It is the safest form of electronic payment offered, and except for the disincentives and dislocations in the marketplace produced on behalf of signature-debit, PIN Debit would be the predominant way to pay in the U.S.—just like it is in the rest of the world.

In this document we will analyze how the availability of PIN Debit for ecommerce transactions brings the benefits of PIN to the Web, namely a reduction in chargebacks and fraud that benefits all stakeholders across the payments value chain.

We will look at different approaches that have been developed to bring PIN to the Web, namely PIN equivalent options and software and hardware encryption.

An in-depth examination of a software encryption solution, PaySecure, will demonstrate that a solution for Internet PIN Debit that has been developed and rolled out in the US to thousands of FIs, supports the Fed's rulemaking objectives.

At this critical point in the rulemaking process the Fed is in a position to influence the adoption of this technology by:

- Issuing technology specific standards for Internet PIN Debit
- Allowing issuers to collect a fraud adjustment for implementing Internet PIN Debit
- Mandating Financial Institutions to carry at least one network that enables internet PIN Debit.

A Brief History of Debit Card Use Online

A common view of the online payment marketplace suggests a sustained effort by the U.S. banking industry to avoid introducing PIN Debit to eCommerce, despite the natural and effective solutions it has offered it for more than a decade. Some of the factors influencing this development have been:

- *Card Not Present rules applied to online debit card use.* While eCommerce was predicated on the credit card in the mid-1990s, by the early 2000s, many key participants were searching for ways to bring Internet PIN Debit in order to address the exploding problem of fraud and charge-backs. Bank card association rules for Card Not Present

(CNP) transactions for mail and telephone orders were extended to eCommerce, putting the onus of risk management squarely on the backs of merchants, and bank risks were further mitigated by higher interchange rates and one-sided charge-back policies.

- *Signature-debit card use eclipses credit cards.* Visa's signature-debit card transactions online exceeded credit card volumes by mid-2005, but merchant investments in their own risk management platforms—rather than bank card associations' security initiatives—s succeeded in limiting fraud to a manageable level as far as banks are concerned but at a steep and unnecessary cost of doing business for merchants. In the process, a number of worthy experiments and tests with PINs online that could substantially reduce billions in fraud costs a year fell by the wayside.
- *Efforts waged to avoid PIN Debit use.* Some of the efforts by the bank card associations and their member banks to forestall the use of PIN Debit payments online were overtly uncompetitive, such as initial prohibitions on PINless debit for online bill payments, which had to be rectified by the Department of Justice. Others were simply discriminatory, such as offering consumers 'zero liability' for signature-debit card transactions, but not for safer, cheaper PIN Debit payments.

Despite these obstacles, Internet PIN Debit has emerged. It took some forward-looking EFT network veterans to support the premise that digital technology properly designed and implemented could actually *reduce* the risk and incidence of fraud, rather than increase it. A decade of preference for signature debit shown by the banking industry, surcharges on consumers for PIN Debit use, and policies and rules that promoted the use of much-higher interchange rate signature-debit has not killed off the high potential for securing online commerce and banking the way PIN debit has offline.

PIN Debit Options Online

PIN Debit payment options can and do work in remote transaction venues such as the Internet and mobile. Meanwhile, through intense marketing that has persisted most of the past decade the bank card associations have promoted alternatives for secure e-commerce payments, namely 3-Domain Secure (e.g., VerifiedbyVisa, SecureCode by MasterCard). However, despite these efforts, adoption has barely reached 10% of the card base. There are, however, alternatives available that have gained traction in the marketplace:

- *Software-encryption emerges as preference.* PIN Debit options that encrypt the PIN with sophisticated software have made steady progress in the U.S.—and one provider (Acculynk) now counts nine of the top 12 EFT networks, card payment networks MasterCard and Discover as partners, and with several processors

adopting it, it is becoming a de facto industry standard. More certifications are expected soon.

- *Hardware-encryption options have had only limited success.* Hardware-based encryption options were tried in the U.S. several times in the early 2000s, and have been only modestly successful in Europe and elsewhere. The extra requirements and regimen to obtain, install and use secure PINpads connected Internet-accessing devices has proved to be a daunting constraint to adoption.
- *'PIN-equivalent' options trying to fill natural vacuum of PIN Debit.* Some PINless and other 'PIN-equivalent' variations for debit account access online have arisen out of the need for more secure and cost-effective debit account access than signature-debit. A number of them in the U.S. mirror the so-called 'credit push' alternatives that have proven fairly popular in areas like Denmark, Scandinavia and Canada, although consumer and merchant traction have been limited.

Need for Internet PIN Debit is validated. The persistent pursuit of a better debit 'card' solution for remote transactions validates the need for PINs online. Each set of options has distinct tradeoffs, but each is significantly better than signature-debit as an online payment mechanism. And all have had to operate under the artificial pricing 'bubble' that signature-debit (and mag-stripe economics in general) impose—i.e., if online merchants are forced to take mag-stripe cards for the fo*reseeable fu*ture, incorporating PIN Debit will only save them money on incremental transactions. The real break-through in reducing risk and fraud costs for all parties will come fundamentally as PIN Debit *replaces* signature debit.

Benefits of Internet PIN Debit

Internet PIN Debit provides substantial benefits for consumers, merchants and financial institutions. PIN Debit is the one payment option that can benefit all parties in payment (excepting those consumers who game the system with friendly fraud):

- *Consumer value proposition.* Consumers get a reliable purchase from a payment mechanism they trust and are familiar with. They know that payments will generally process right away and be successful.
- *Merchant value proposition.* Merchants save substantially from reduced costs on repudiated transactions and handling of extraneous charge-backs. These cost savings typically get passed on to consumers in terms of lower overall pricing.
- *Bank value proposition.* Banks also save considerably with a Internet PIN Debit transaction, vis-à-vis signature-debit, in the reduction in charge-backs and related customer service costs. They will also benefit longer term from reduced charge-offs from DDA accounts that go bad due to authorizations and fees on overdrafts.

Payments 'ecosystem' benefits overall. Secured PIN Debit, coupled with dynamic data authentication and encrypted account credentials generated by the EMV (or other) chip (in a card or a mobile handset), can remove the bulk of the fraud from the payment system. As well, in mobile venues, use of PIN Debit can help usher in a new era of two-way communications between buyers and sellers in a secure, digital format with Near-field Communications (NFC) by augmenting (with user verification) the use of digital IDs and unique mobile transaction identifiers for second-factor authentication in online (and offline) transacting.

Optimal Configuration

A hosted PIN Debit interface between merchants, consumers and EFT networks delivers both security and efficiency; the 'floating PINpad' is the best user convention for PIN entry. A decade of experience demonstrates that the following components of a Internet PIN Debit system produce optimal results for the payment ecosystem:

- *Hosted system design optimizes security and efficiency.* The process for using Internet PIN Debit is relatively simple—no terminals are required—just software to access the secure host. Merchants need only offer PIN Debit as an option on their check-out pages with links to the host; the host then presents the floating PIN-pad to the consumer's browser (or mobile handset screen). Once the PIN is entered into the software and transmitted back to the host, the host routes the authorization request to the designated EFT network. The EFT network then decrypts the information (which includes a unique transaction ID generated by the host), and processes the authorization (and settlement) just like any POS transaction (check this for accuracy!). Merchants have little to do; consumers need only familiarize themselves with the interface, and issuers have nothing to do at all.
- *Special situations CAN be accommodated.* More importantly, demonstrable solutions for online purchases, bill payments, peer-to-peer payments and remittances, T&E, and 'staged' ordering all exist and will scale to national and global use. The key to avoiding more fruitless investments in mag-stripe, and signature-debit in particular, is gaining a commitment, perhaps led by the Fed, to moving to a new payments paradigm, in which PIN Debit will work as naturally and effectively in the online and mobile venues as it does at POS (when it has been allowed to participate).
- *Configuration supports Fed Rulemaking Objectives.* This Internet PIN Debit solution can function to foster compliance with the core Rulemakings in four ways:
    - *Debit card interchange.* Efficiencies built-into existing ATM debit card processing environments are leveraged in expanding to Internet PIN Debit—helping enable issuers and processors to earn profits under newly proposed rates

- *Fraud offset.* Internet PIN Debit clearly satisfies the implied standard for fraud adjustments, giving issuers a chance to earn a fair return for enabling Internet PIN Debit, and EFT networks an efficient new source of safe volumes
- *Debit network competition.* A hosted system can channel PIN Debit transactions to multiple options for EFT authorization and processing, fostering network competition (including consumer and/or merchant choice in the front-end) and ensuring network interconnectivity options in the back-end
- *Small FI exemption.* Ubiquitous access to all financial institutions via the host system enables any enabled bank or credit union—including those under the $10 billion asset exemption—without any separate infrastructure investment.

Value of extending PIN Debit to other payment types. The potential value of securing PINs in digital venues extends well beyond its logical role as a supplement (and likely replacement) for signature-debit, provided that its deployment is coordinated within an overall plan for migration of debit account payments. Such extended use of PINS for securing payments include credit cards, ACH transactions, and general purpose reloadable prepaid debit cards, as well as new application areas such as health care uses, government identification and licensing, and even voting.

Benefit of making PIN Debit the preferred debit card payment type. The numerous deficiencies of signature-debit create a motivation to move primary debit card use to the more efficient and cost-effective PIN Debit, as exists worldwide. The key to attaining the benefits of PIN Debit's rightful place at the heart of secure payments is communicating a consistent path to the desired end-state for 21st century transacting.

Fed Rulemaking

The Fed has requested comment on rulemaking as the provisions of the Dodd-Frank Act with regards to EFTA Section 920 are rolled out. At this critical point in the rulemaking process the Fed is in a position to influence the adoption of internet PIN Debit through several tools:

- *Fraud Adjustment*
  - Issuing technology specific standards for Internet PIN Debit
  - Allowing issuers to collect a fraud adjustment for implementing Internet PIN Debi
- *Network Competition*
  Mandating Financial Institutions to carry at least one network that enables internet PIN Debit.

2. Historical Background

An examination of the progression of the eCommerce marketplace suggests that the use of Internet PIN Debit has systematically been avoided by the banking industry for more than a decade—despite the sizable improvements in reducing both friendly and unfriendly fraud.

Remote transacting follows card paradigm. eCommerce began in mid-1990s based on the four-party credit card model (cardholders, issuing banks, merchants and acquiring banks), largely because it was an electronic form of payment used by nearly three-quarters of adults in the U.S.—the primary initial market. But there were great concerns from the outset that this venue would expose the payment system to substantial new risks; some of those risks were first manifested a decade before as the mail order/telephone order business (known as MO/TO), which was mostly based on credit cards in the early days, grew to a $150 billion a year business by the inception of eCommerce.

Higher rates of fraud in MO/TO. Among the problems experienced with MO/TO was a higher rate of fraud, as merchants could not verify that the presenter of the card account credentials was the legitimate owner of the account in such remote, non-face-to-face circumstances. In time, merchants would seek other identifying information, such as addresses and telephone numbers, but charge-back incidence continued to grow along with the market. Other problems experienced in MO/TO transacting included the ability of cardholders to repudiate transactions, claiming that the cardholder information, primarily the Personal Account Number (PAN) and the expiration date and name of the accountholder—all embossed on the card in plain sight, must have been provided to the merchant without authorization. The merchant had little in the way of proof at first to dispute the charge-backs that resulted, and thus the practice of 'friendly fraud' emerged, where consumers would know a transaction had been conducted—by family-members or friends or even themselves—and had actually received the disputed goods, but would deny either or both, and launch a charge-back against the merchant. By 1995, MasterCard data indicated that charge-back rates were 10-15 times higher for MO/TO business than for POS transactions, and that fewer than a million cardholders produced more than 60% of charge-backs. So-called charge-back 'recidivism' had quickly joined real fraud—which was much, much easier to commit remotely, at virtually no risk of getting caught to the perpetrator—as a threat to the payment card system.

eCommerce relegated to Card Not Present domain. During the first decade of MO/TO, the credit card companies came to define remote transactions as "Card Not Present" (CNP), adopting and promulgating specific rules (such as charge-back rate ceilings, or thresholds), higher rates (about 80 bps over POS average interchange), processor risk mark-ups (some smaller remote

merchants paid up to 5-6% discount fees in total), and liability policies (basically, the remote merchant bore all the fraud unless the purchase could be uncontestably validated). In effect, if merchants wanted to conduct remote transactions, they did so at their own risk, and at rates that ensured the banks and credit card companies would be fully compensated for any risk or additional costs to the system. It was the CNP domain that eCommerce was transitioned into from the outset.

Associations develop their own security protocols. Online fraud was viewed in the mid-1990s with great trepidation, however, given how quickly large volumes of account credentials could be compromised and exploited electronically.

- S.E.T.: Visa began an effort to augment card security online in conjunction with Microsoft in 1994; under the initial design, Microsoft would provide digital Visa account 'credentials' in encrypted form, in return for a reported $.04 per transaction 'commission'. MasterCard countered with its own digital certification initiative (with Microsoft rivals IBM and Netscape). By the end of 1995, the big banks 'ordered' Visa and MasterCard to consolidate rival efforts, and the result was Secure Electronic Transaction (S.E.T.) protocol Despite massive marketing efforts and hundreds of bank pilots around the world, SET never took off; it was too expensive to build out a digital certification system for all four parties, and the computing power of the day meant additional authorization times of more than 30 seconds—an unacceptable delay for consumers. SET floundered for a few years, before Visa decided to eliminate the cardholder certification requirement. The result was 3-Domain Secure (3D Secure), which emerged in the early 200os as VerifiedbyVisa and SecureCode.

- *3-D secure flounders, too.* Ironically, by eliminating the cardholder identification/verification component, the bank card associations 'built-in' the problems the already had with both real fraud and friendly fraud. That, and clumsy deployment policies with minimal rate relief or financial incentives forestalled merchant adoption for many years. Today, 3D Secure covers less than 10% of card transactions, and is widely viewed as ineffective security—while the world clamors for a better solution—preferably utilizing PIN Debit in order to replicate marketplace usage and curtail the fraud problems.

PIN Debit alternatives surface to address real problems. PIN Debit experiments (mainly with hardware encryption) were tried in early 2000s, but experienced a difficult time cracking the closed card payments market:

1. Hardware option with banks/etailers. In 2001, Amazon, eBay, Citibank and Wells Fargo held a number of meetings to design a new PIN-based debit payment capability using secure PINpads to be plugged into mainly home computers by consumers; the functional and technical designs were completed, and critical mass adoption was expected given the

dominance of the Internet's two biggest merchants, but the coalition fell apart when the two banks could not agree on what to charge the merchants for online transactions.

2. *Hardware options with EFT Networks.* About the same time, eight of the EFT networks met repeatedly under the auspices of consulting firm to try to come up with a PIN debit solution. They managed only to define rules and standards, but not an optimal product. Another effort, initiated by NACHA, the Automated Clearing House rules-making body resulted in a proposed mechanism called the Internet Secure Access Protocol (ISAP); this envisioned PIN Debit transactions 'pushed' from online merchants accompanied by a secure token (using Public Key Infrastructure, or PKI). Another experiment by a leading EFT network involved extensive testing of a plug-in secure PINpad to generate encrypted PINs. The hardware had been used with modest success offshore, but failed at both user convenience (perfecting the installation) and reliability (executing transaction throughput); so the initiative was abandoned despite a fair amount of publicity and support. None of these efforts producing a workable solution for PINs online—largely because of their inherent deployment complexities—but they demonstrated the sustaining interest in doing so.

3. Hardware option—CD-ROM with NYCE. In 2003, the EFT network NYCE introduced its initial version of Safe-Debit. This version utilized encryption algorithms that scrambled PIN Debit account credentials on a 20MB Computer Disc. The CD, which was distributed by member banks, had to be inserted into the PC, would present the encrypted credentials during an online purchasing session to the authorizing network. While again demonstrating the growing capabilities of software encryption, the hardware requirement as a user interface proved unavailing; the SafeDebit pilots foundered from lack of adoption by consumers, merchants and banks. By this point, the 'chicken-and-egg' conundrum began to be regularly applied to any new payment vehicle that emerged, and many began to doubt that any hardware option would catch on with consumers.

4. Software-encryption of PINs gains steam. By mid-decade, efforts to put Internet PIN Debit shifted to software-encrypted products, which were thought to be much easier to deploy, but still far more effective in reducing fraud than anything the bank card associations offered.

5. PIN-authenticated ACH. In 2004, one of the industry's biggest processors proposed implementing an Internet-specific payment capability that used online-only PINs for ACH cleared-and-settled transactions. The system would utilize encryption software, and smart browsers or downloadable clients for user PCs. Extensive consumer research suggested that one in four online transactions would be made by this mechanism if sufficient bank and merchant adoption was achieved, especially new and increased usage by consumers

worried about Internet security. After a considerable investment, the project was tabled for several years—partly out of concerns that it competed with the processor's substantial signature-debit card business, and failed to leverage its PIN debit network.

6. *'Floating PINpad' gets a new partner.* That same year, ATM Direct—the predecessor to Acculynk—assembled relevant patents and launched small pilots to demonstrate its 'floating PINpad' technology. These proof-of-concept initiatives were carefully scrutinized by several EFT networks, several of which were now owned by big processors, but concerns about cannibalizing signature-debit and whether PINs could be properly protected stalled further progress—despite considerable merchant interest. At the time PIN Debit interchange rates were less than one-fourth of signature-debit rates at POS, and merchants expected similar savings would result for online transactions.

7. 'Credit-push' variations and email payments surface. Other alternatives, built around signature-debit pricing, soon took center stage.

- *NACHA offers ACH option.* NACHA's credit-push initiative (now called Secure Vault Payments, or SVP), enabled merchant websites to redirect consumer browsers to their online bank for authentication. The online bank then passed an approval code back to the merchant, and paid the merchant offline via ACH. eBillMe (an offline version of SVP) surfaced soon after. And even some products that performed second-factor authentication for Internet purchases using mobile phone confirmations by voice and PIN emerged.

- *PayPal becomes the alternative payment leader.* By 2005, PayPal, which used a second log-in as a second factor for authentication (PIN entry is also a second factor, but much stronger) had emerged as the first successful alternative payment, with a 5% share of the market (it reports a share of more than 15% today); PayPal offered merchant accounts small, but significant reductions in conventional discount fees, and somewhat better charge-back protection—proving that even a little relief from conventional practices, deployed via a software mechanism that requires only a second log-in (even less work for the consumer than PIN entry), can win widespread consumer and merchant support. Since 30% of PayPal's account loadings came from ACH, in effect, it was a debit account payment option. Thus, the shift from an emphasis on anti-fraud to a marketing push for higher interchange signature-debit took center stage—ceding the online opportunity largely to PayPal.

Analysts and researchers proclaimed inevitability of Internet PIN Debit. And such an outcome defied conventional industry wisdom. In 2006 and 2007, research reports by Celent and Mercator Advisory Group speculated on the inevitability of Internet PIN Debit, citing consumer and merchant preference, but emphasizing its much-needed (and much delayed) importance in

reducing real and friendly fraud. Software-encryption solutions were advocated as the most effective deployment alternative, and expectations were that the new processor-owners of the big EFT networks would eventually make Internet PIN Debit happen.

So efforts to figure out some way to bring PIN Debit to the online venue resumed. Though software-encrypted PIN Debit solutions have finally begun to gain some traction, hardware-based solutions appear to have stalled out. The incremental cost ($50-100 per user), the hassle of installing and setting up the readers, and uncertain consumer usage/adoption has all but exhausted the ability of the handful of providers to continue operation. HomeATM, a Canadian company, has few customers outside of high-risk (i.e., adult and gaming websites) merchants; the same is true for UseMyBank, NetTeller and other providers.

Bank and Association resistance continues. The implied threat of bringing PIN Debit's lower interchange at POS to the online market as well as offline appeared to shift the banking industry's strategy to eliminating this potential threat to high signature-debit card interchange. By 2004, led by Visa's Interlink, PIN Debit rates began an upward trajectory that, by late 2010, eliminated nearly all the advantages PIN Debit had over signature-debit interchange. The other EFT networks, in order to retain issuers, eventually followed the Interlink progression to virtual rate parity.

Though most industry veterans acknowledged and defended the superior security of PIN Debit, the banking industry pushed signature-debit seemingly every way they could. By the early-2000s, the 'zero liability' program begun with consumer credit card use was extended to debit cards; coupled with the public's growing preference to use debit cards rather than credit cards in general, this blanket protection helped generate soaring use of signature-debit online. By 2005, Visa reported more signature-debit card transactions online than credit cards. An unfortunate bi-product of such policies, where online merchants were liable for nearly all fraud, was soaring rates of transactions repudiated by consumers, and so-called 'friendly fraud'.

In the meantime, banks rallied around the higher signature-debit interchange rates and focused their loyalties and marketing dollars on that form of payment. As well, up to 20% of banks applied surcharges (of $.25-$.75 per transaction) if their customers used PIN Debit for purchases, according to the U.S. Public Interest Working Group studies..

Such policies discouraged any real competition in online payments. By 2010, even powerful companies like Google and Amazon could not make much of a dent in the signature-card payment dominance online. Although various research reports maintained that one in five Internet purchase transactions were done by 'alternative payments', most of this volume was produced by PayPal, utilizing existing banking network interconnections. Even when true alternative payment options managed to gain trials and toeholds in the market, pricing was generally targeted to

signature-debit rates, less a small discount of about 20-25 basis points to tempt merchant adoption.

3. Alternative Online Payment Options

3-D Secure

3-D Secure appears unlikely to serve more than a small fraction of the debit card market due to several factors:

- *Limits on Visa's penetration.* A Visa executive told a merchant risk group in 2008 that VerifybyVisa would never be used on more than 10% of its transactions globally.
- *Limits on MasterCard's penetration.* In Belgium, where MasterCard Maestro is the domestic debit card, and SecureCode enjoys its highest penetration, but only 14% of online transactions were protected by this mechanism, according to recent report..
- *Uneven merchant value proposition. W*here merchants have weathered the oftentimes confusing and frequent deployment updates in order to embed 3-D Secure into their web transaction *servers, and consumers have agree*d to go thr*ough some sort of auto-enrollment p*rocess, the extra log-in protection can be relatively transparent. Generally, merchants can save 5 bps in interchange (59 bps if they fully deploy SecureCode in the html layer for added transaction validation).
  - *Man-in-the-middle attack vulnerability.* But any secondary log-in protocol is subject to 'man-in-the-middle' attacks—including 3-D Secure—where a compromised transaction, even with account credentials still encrypted, can be replayed for a fraudulent purchase.
  - *Security lacking.* The log-in security for 3-D Secure is typically outsourced in the U.S. to third party companies, and meets most banking standards, but the general lack of adoption attests to the marketplace's lack of confidence in these protocols for safeguarding the build of eCommerce
  - *Operational issues.* Operational issues were so common in the early going that the 5 bps rate reduction was given to merchants if they even *attempted* to do a SecureCode log-in. While most of those operating issues have been ironed out, merchant experience has remained very disappointing. The original quest of reassuring security-conscious consumers that the Internet is safe to transact on has been little served by the presence of 3-D Secure. Moreover, the auto log-in feature that provides the transparency does nothing to prevent a stolen laptop (or other claimed compromised device) from being an instrument of repudiated transactions; a secondary process of secure PIN entry is not provided.
  - *Consumer experience erratic.* Consumer experience at times has been very bad, as discussed above. But the effort to make the secondary log-in transparent, also discussed above, has in effect devalued the attempt at portraying additional security. And the 'zero liability' marketing and related policies have done nothing to weed out the charge-back recidivists. By contrast, the experience with Internet PIN Debit has consumers gratified by the familiar (and reliable) security mechanism and shopping more confidently.

- *Bank experience disappointing.* Bank experience with SecureCode has been troublesome at times as well, and the fact that most of the 3-D Secure issuer authorization is largely outsourced speaks to the fact that many bank issuers have not acknowledged that there is justification for bringing the processing in-house. As well, most of the markting efforts to induce consumer enrollment and to get merchants to adopt the protocols have materially subsided. As a consequene, the online marketplace still lacks a bankcard solution that has any meaningful impact on fraud, or relevance to transactors.

Hardware encryption

Hardware encryption solutions are expensive, and too hard to install and operate. An early example was provided by the Amex Blue Card. As widely reported, when American Express introduced the Blue Card in 1999, amidst a high-tech marketing strategy that depicted the card being stretched in different directions (signifying its flexibility in functionality), expectations were high that this would be the solution for scary remote commerce. Some 50,000 smart card chip readers were distributed to customers free-of-charge. But due to installation complexities and lack of consumer motivation, only about 5,000 were actually taken live, and before their use was terminated, only a handful of actual transactions over the Internet transpired. While Blue Card turned out to be a successful marketing program, as a secure payment mechanism, most of the world concluded that a hardware solution would never attain critical mass.

Most hardware based security, including computer chips, turn out to be pretty effective; i.e., good security, but too difficult to deploy and too expensive to finance. Since that time, any hardware solution for consumer use is generally doomed to failure. And deployment of hardware plug-in devices remains a difficult task, requiring substantial investments in consumer education, online or other training, customer services, repair and replacement, etc. Meanwhile, throughout the 2000s software encryption techniques got stronger, more efficient, cheaper, and much 'lighter' to deploy—including the ability to run on devices as small as mobile phone.

Merchant experience with hardware encryption systems requires not only the ability to pass the 'tokens' through transaction systems (something PCI compliance demonstrates is a major task), but helping the consumer with operational problems that they tend to blame on the merchant. ROIs for deploying such complex systems are impossible to derive unless and until critical mass adoption occurs. So merchants tend to have little interest in supporting payment options that are inherently complex.

The consumer experience with downloading client applications has become both familiar and effective over (e.g., a reported 130 million anti-virus programs have been deployed), but this experience has been further simplified by accessing security through host systems ('in-the-cloud') and in Software-as-a-Service (SaaS). So the idea of adding software to a device to protect it, and any credentials stored on it, has become commonplace. Further, mobile phone application

downloads exceeded 10 billion by the end of 2010. Downloads are quickly becoming how digital lifestyles are lived.

The most common way to generated hardware tokens to augment security comes from smart cards; more than a billion chip-secured payment cards have been issued around the world. In the 1990s, U.S. banks conducted a number of pilots of smart cards, distributing thousands of smart card readers at POS, effecting authorization of chip-generated tokens, issued hundreds of thousands of cards with chips, and promulgated dozens of types of chip-reading devices to cardholders. Needless to say, none of that investment paid off.

Perhaps the only relatively successful bank experience with hardware deployments has been authenticating devices (e.g., those generating new six-digit numbers every 60 seconds) for commercial accounts doing wire transfers and online banking. And even those bedevil bank customer service and support operations. So banks remain very skeptical of hardware deployment.

PIN equivalent options

PIN-equivalent or -substitution solutions exist, but don't appear to scale in terms of consumer or online merchant adoption.

One Time Passwords

Probably the most broadly tested example was one-time-passwords (OTP). In the mid-2000s, Orbiscom and Cyota, among others, convinced a number of banks and networks to support merchant applications that generated a single use account credential (e.g., a PAN and expiration date). Early versions required consumers to be redirected to a different website to procure their pseudo-account credentials, and was barely used. Subsequent deployments were easier and more successful.

A few years ago, PayPal conducted a pilot using OTP MasterCard pseudo-numbers, accepted at any website that offered MasterCard payments, as part of a "virtual debit card" application. After downloading and installing the application, whenever a checkout page was accessed on merchant website, a full MasterCard account credential was generated and filled-in on the payment page. A reported four million of these virtual debit card applications were downloaded and used. This trials was clearly more successful than any hardware implementation to-date, so the OTP alternative persists today:

About a year ago, NYCE re-released SafeDebit using an OTP application, but participation by member banks has been minimal to-date, and volumes are reported to be quite low. STAR, the

EFT network owned by First Data, now offers a product for cards or contactless use that generates a one-time password with each PIN Debit transaction—eliminating the need to enter a PIN. STAR's implementation with OTP is limited to contactless transactions at POS at present, but is intended to support Internet access to the STAR host for online and mobile transactions. This deployment offers chip-based generation of tokens, so it a hybrid between hardware and software security; but it remains to be seen how it will work online and whether users will be as comfortable with the eventual interface as they are with PIN-entry.

Cardholder Verification Number

Meanwhile, one of the most successful tweaks the bank card associations introduced for remote payments is the addition of a three-digit number printed in the white signature stripe on the back of the card. Known as a cardholder verification number generically (but usually called CVV2 for Visa, CID for Amex, and CVC for MasterCard), this number is just a three-digit PIN; but it is printed on the card, visible to any authorized—or unauthorized—possessor of the card for submission of payment credentials. And it only attests to the fact that the user actually had possession of the card at one time—not necessarily for the transaction at-hand. Again--just a partial solution from the associations that misses the full potential of PIN Debit robustly implemented online.

Other debit-account solutions and credit push options

Other debit-account solutions tend to be specific to individual nations, and don't scale globally (e.g., browser redirect to online bank, credit transfers, etc.), but continue to be plumbed into the infrastructure, mainly out the lack of an effective PIN Debit solution that can be embraced by card issuers. This situation is particularly ironic, since most of these countries are so PIN debit centric in card use.

For example, credit-push payments, where the consumer's browser is redirected from the merchant website at the checkout page to their online banking website for separate authentication, can either be done out-of-session (as with eBillMe) or within the session (as with NACHA's SVP or Mazooma). Consumer, merchant and bank take-up of these mechanisms has been very modest to-date. In Canada, where a conscious decision was made by its PIN Debit network, Interac, to avoid PINs online (and four private companies have tried to get traction with credit-push types of payments services without much success), Interac's version has experience miniscule use.

A major limitation of these credit-push alternatives is the inability to use them for cross-border purchases. In the European Community such purchases are often 40-60% of total eCommerce within a given country, but lack of payment (and related fulfillment) capabilities results in less than

30-40% of international transactions being approved and permitted if signature-based cards are not used.

Another limitation is the reliance on accessing an online banking system. After more than a decade of existence, online banking exists at only 7,000 of the 16,600 financial institutions in this country. Of those 7,000 deployments, the vast proportion are provided on common platforms, such as those offered by Fiserv, FIS, Online Resources and others. When an individual financial institution decides to offer online banking, it must choose from a limited selection of standard, undifferentiated services supported commonly on the platform. While this facilitates a common deployment path, it also constrains the choice of when and how to offer more innovative choices. So it is no surprise that PayPal's current strategy is to become the default online payment option for any bank offering online (or mobile) banking—since these banks are largely unable or unwilling to offer payments directly. (The business model is that the vast proportion of smaller banks have little or no signature-card use online, so agreeing to steer their customers to PayPal transactions, where they get a $.25 commission, is nearly all upside for them.)

PIN Debit, on the other hand, is supported by almost every financial institution in the U.S., since ATM access is nearly universal. (ACH connections are also almost universal among financial institutions, and work well for bill payments—which are also 'pushed' payments—but not for purchases). If a common solution were available for doing online purchases, and not limited to online banking platforms, *every* bank and credit union that offered Internet PIN debit would stand to benefit.

Conclusion of evaluation of different on-line payment options

In sum, despite the clear global preference for secure debit account access for online transactional services, very little protection is available to-date. Meanwhile, eCommerce volumes continue to grow (15% p.a. over the past five years), encouraging repeated efforts to build and try new payment alternatives that fill the PIN Debit gap. Yet research continues to show that a significant portion of the population still avoids shopping online because of security and privacy concerns, and transaction abandonment rates persist at 50-65% rates, in no small part because shoppers cannot make their purchases with the payment instrument of their choosing.

Alternative payments, as discussed above, tend to fit only small niches as consumers and merchants are reluctant to try out unfamiliar products. The only successful provider (PayPal) is really just arbitraging bank networks with a dual log-in format, but ironically leverages debit account access for funding their stored value accounts in ways the banks themselves do not provide. According to the company, some 30% of PayPal account loads are done via ACH, where access to consumer debit accounts is enrolled prior to using the bank account. Last year, PayPal extended debit account access by incorporating a STAR PINless debit loading function—which

offers the alternative payment provider even more reliable account loads. So, apparently at least one payments company has figured out how to make online debit account access work without exclusive reliance on signature-debit cards.

Innovation by private companies on top of banking networks has extended to peer-to-peer payments over the past year. Two of the prominent P2P providers, PayPal and Obobay, basically just invoke a staged account opening and verification process to allow consumers to access their bank debit accounts—something banks could easily do themselves, if there was any motivation to do so.

Other transacting venues, such as T&E, split or staged-order businesses, and mobile, still only have signature-card payment options in the main, and suffer significant overhead from authorization declines, multiple authorizations, transaction cancellations and reversals, charge-offs, and the like. More importantly, orders are often submitted in batches, with delays, to conduct ancillary risk management checks. PIN debit solutions are no more complicated than signature-debit, but come with far less overhead and the ability to ship orders right away.

As a consequence, online and mobile venues remain frustrated and desperate for more efficient and effective (i.e., real-time, guaranteed, non-repudiable) debit account access, and their digital nature has enabled them to become a laboratory of experimentation for new payment types and authentication protocols that often use banking networks to facilitate innovations that the banks themselves will not. For the most part, though, dozens and dozens of these experiments have come and gone, while consumers and merchants largely hold out for a serious PIN Debit alternative.

4. Benefits of Internet PIN Debit

When the benefits to all parties in a payment transaction are weighed, PIN Debit is the right solution for online use—just like it is at POS. But the deployment of Internet PIN Debit is much simpler and far less expensive than offline build-outs, and address the overall goals of the Durbin Amendment Rulemakings in substantive ways.

Simple, convenient and safe on-line payment tool

The process for using Internet PIN Debit, as embodied in Acculynk's PaySecure product, is relatively simple—no terminals are required—just software to access the secure host. Merchants need only offer PIN Debit as an option on their website check-out pages, with links to the host; the host then presents the floating PIN-pad to the consumer's browser (or mobile handset screen). Once the PIN is entered into the PIN pad, the software captures the geo location (x/y coordinates) of the number entered by the consumer and transmits them back to the host. The patented algorithm then translates the variable into a PIN, assembles a PIN package and routes the authorization request to the designated EFT network using standard ISO 8583 messaging. The EFT network then decrypts the information (which includes a unique transaction ID generated by the host), and processes the authorization (and settlement) just like any POS transaction.

Merchants are enabled for the product through their acquirers and can integrate the solution with minor effort; consumers need only familiarize themselves with the interface, and issuers have nothing to do at all—a big advantage in a post-Durbin restructuring of debit card economics and use. In normal, competitive businesses, the PIN Debit solution is logical, natural and desirable; in a signature-debit dominated online market, it has taken a decade to get even a foothold.

Marketplace Acceptance:

EFT networks and merchants

A recent study by one EFT network found that the floating PINpad was preferred by more than 80% of online merchants, which viewed it as the most familiar way for consumers to get used to doing Internet PIN Debit. Merchants see a wide range of benefits**:**

- Fraud and charge-back savings accumulate as each signature-debit purchase is replaced with a PIN Debit purchase. Over time, as mag-stripe usage overall fades in concentration of purchase volumes, these savings are augmented by the ability to reduce the amount of investment Internet retailers must make to stay ahead of fraudsters and reduced exposure to PCI compliance costs
- Lower incremental investments in risk management technologies are required. Generic use of a payment option such as Acculynk means less need to invest in elaborate risk management systems (e.g. Accertify, ThreatMatrix, 41st Parameter, etc.)

- Concomitant ability to steer payment choices to safer, more cost efficient options like PIN Debit reward the merchant for adoption, and produce a return-on-investment much faster
- The ability to add competitive network options for each debit card purchase, as contemplated in the proposed rulemakings, can be augmented by a host-based system that enables EFT network brands in addition to signature-debit brands on the check-out page
- From a performance standpoint, fewer shopping carts will be abandoned and more transactions will be completed with the addition of a generic PIN Debit option online
- Cross-border eCommerce will be facilitated. Far more international transactions will be possible as PIN Debit systems are supported in more countries with most merchants. The near-instant settlement properties of PIN Debit can also expedite order completion and fulfillment, speeding up product and service delivery—something even merchants could charge fees for to offset their minor costs of deploying Internet PIN Debit.

This same survey of 20 banks and credit unions produced nearly the same level of support for the floating PINpad user interface, and indicated that PIN Debit was a necessary and desirable option—provided it could be as secure as POS transactions. A growing number of banks are embracing Internet PIN Debit for economic and customer loyalty benefits:

- Signature-debit is high-cost to banks. Those banks that do conduct an appreciable amount of online transactions are known to experience substantial costs in charge-backs, charge-offs, and customer service expenses for all the things that go wrong with signature-debit payments. Shifting to PIN Debit will not lower those mostly fixed costs (like the big merchants') right away, but over time, the savings will begin to mount.
- Switching to PIN Debit can help banks earn a profit on lower interchange rates. This benefit can be an important component for them to get to a point where they can actually make a profit on a $.12 interchange fee ceiling for debit cards; on the contrary, it is likely that signature-debit card transactions produce at least $.05-$.15 in extraneous costs per transaction that the banks now have to absorb without passing onto the merchants.
- Less real fraud, along with a tool to combat friendly fraud (and begin to manage down chargeback recidivists) and unravel the collateral 'zero liability' costs they incur
- Reduced incremental charge-back/customer service costs (typically estimated at $15-25 per complaint-handling call)
- Potential to capture business of customers who are currently reluctant to shop on-line due to security concerns
- Potential to capture spend from non-bank branded alternatives (e.g. PayPal)
- Enabling of ATM-only cards (about 12% of all debit cards nationwide, according to some EFT networks) to shop online.
- Fewer cases of online data breaches, with minimal exposure to man-in-the-middle and replay attacks

- Possibilities of working with merchants and their data to embellish compensatory controls (e.g., limits for new customers, but incentives for expanded use)
- Possible additional interchange permitted by the Fed for investment in Internet PIN Debit deployment

Consumer research consistently demonstrates a desire to use PINs online in as much the same way as at ATMs—namely the floating PINpad interface with interactions managed by a secure host system.

Consumers also say they want to avoid having to pick or scroll through a lengthy menu of selections in order to choose their debit-card bank provider, when a simple EFT network choice would automatically result in the standard BIN-sort (on the first six digits of the PAN, which designate the bank electronic address as the 'Bank Identification Number') with no work on the consumer's part. So consumer adoption—which so far has proven quite painless (some 56% of consumers, when apprised by the merchant website that they are doing a PIN Debit transaction, go on to complete the transaction) and quite encouraging.

Security improvement provided by Internet PIN Debit

Security is substantially better than any debit account alternative, and acknowledged by both consumers and merchants (as well as some EFT networks and banks). Acculynk, for example, has been vetted by nine EFT networks, as well as MasterCard, Discover, and First Data. (A security assessment by Pulse—part of Discover—is quite demonstrative, and can be shared under non-disclosure agreement as warranted). Thus, Internet PIN Debit fully satisfies most or all of consumer demands for improved protection for transacting over the Internet. Supplemental features will support achievement of critical-mass and scale in the U.S. and beyond, using available commercial insurance, compensatory controls and other tools. Acculynk's experience to-date (volumes are not huge yet, since EFT network adoption has mostly come in the past 1-2 years) is encouraging, with 40 million debit cards enabled to use the service. This experience has produced no fraud, making it even safer than the PIN Debit experience at POS, which Pulse surveys consistently show PIN to incur 5-10 times less fraud and charge-back incidence than signature-debit, and an 80% reduction in chargebacks.

Product features

PIN Debit solutions can be made to work in difficult venues that some inputs to the Fed suggest are not practical for PIN transaction messaging (PIN transactions conduct authorization and settlement in a single message). For example, travel deposits— taking a $250 authorization upon renting a car or checking into a hotel, is currently handled via signature-debit by taking an advanced deposit, where the net charge at the end of the rental or stay is processed, and any remaining balance is reversed. This process takes several days up to 2-3 weeks.

PIN Debit can be used in a similar fashion; and there are alternative constructions that use PIN Debit to effect a hold on the deposit amount, without withdrawing the funds (settlement is suspended for a pre-defined period); when the final amount is known, the hold is cancelled, and the actual amount is authorization and settled. With PIN Debit, the hold is actually a hold, so the funds are actually available when the final purchase amount is withdrawn for collection.

Split shipments/orders, where online merchants cannot fulfill all of the goods ordered (and authorized against) in a stated time-period, can be handled in a similar fashion, with PIN Debit temporary holds (and reversals). In addition, PIN debit use provides much more effective capabilities for ensuring the final charges can be successfully authorized against good funds in the account.

Other Benefits from Internet PIN debit

PIN Debit can drive future, new eCommerce in a productive way. More consumers coming online, shopping, and spending for legitimate transactions will build legitimate volume for the system overall; use of PIN Debit avoids problems inevitable with continuing and expanded use of signature-debit before they ever happen.

Foundation for banks and merchants working together exists. The key for optimizing deployment at this point is to build on the new interchange structure, which puts a hurdle on issuers, but also provides new motivation to help out on reducing online fraud.

- As merchants seek to expand use of lower-cost debit, both retailers will have the motivation to contour the new economics of their payment mix, and work together to reduce use of high-cost, high-friction options such as signature-debit
- Because more than 80% of debit cards issues have both signature and PIN capabilities, the friction from inducing consumers to try their PIN will be minimized
- Larger merchants which have optimized their *existing* signature-based card risk management systems will need pricing incentives to cost-justify steering their customers to PIN Debit
- Smaller and new web or mobile merchants can steer their customers more proactively to PIN Debit via gateways while guiding cardholders away from the less-efficient signature-debit option

Consumer Attractions. Consumers will benefit in general from both the security and efficiency (as well as the familiarity and comfort with PIN Debit) both for U.S. and international transacting. As Internet shopping and retails goes global, the potential for cross-border PIN debit card use (which, by the way, is a major objective of the European Union) will become a growing imperative.

'Unproductive' consumers might suffer. Charge-back recidivists will be made responsible, and hopefully accountable, by restricting use of signature-debit (or, soon, the ability to surcharge signature-based card types) and/or promoting the PIN Debit option-only for known perpetrators. While some members of the banking industry claim issuers police this wasteful and corrupt activity adequately, most online merchants would vehemently disagree. Removing these costs from the payments system would benefit all parties.

Benefits likely to emerge naturally to support PIN use. Online merchants are notoriously competitive and tend to operate on razor-thin margins—partly because consumers have such good access to pricing. Since everyone is ultimately a consumer, better merchant economics from the efficiencies and savings of PIN Debit will inevitably be passed on to consumers as a component of overall merchant economics. Incentives and rewards from merchants to cardholders who use PIN Debit are likely to be another form of consumer i

Online fit will help promote PIN adoption at POS. Perhaps as importantly as the foregoing, embracing PIN Debit use in the online venue not only complements, and helps cost-justify, expanded PINpad deployment at POS—to the benefit of all parties. And it will be an essential part of the emerging mobile open wallet, which will be adopted for transacting in all venues, including POS.

Addressing risk concerns about PIN Debit Online

The Acculynk system has received numerous security audits and certifications over the past five years from networks and processors and its record so far in real transaction venues is remarkably free of fraud. But some EFT networks have resisted putting Internet PIN Debit for perceived security reasons—namely that it will condition consumers to enter their debit account PINs in online environments. Much of this resistance among EFTs appears to be based on 'religion' rather than reason. For example, there are ample safeguards for PIN debit use with respect to phishing attacks. As well, recent data breaches and ATM skimming has compromised far more PIN account credentials than any feasible attacks from encrypted use online could produce.

Because many 30-40-year veterans of this part of the banking business have prided themselves on (and devoted their careers to) preserving the impeccable security record of PIN Debit; they have lived in professional fear over the possibility that this high-performance payment system might actually experience a massive compromise on their watch. So it is not surprising that some would prefer *no* online (or mobile) use—ever.

Fear of consumers entering PINs in the clear for other online venues (e.g., email, phishing, etc.) can be overcome the same way phishing has been in general—i.e., consumer training, recommended use of anti-virus programs, confirmation alerts, etc. The additional value created by a phished PIN is negligible as a fraudster in possession of a stolen PAN and expiration date can already make eCommerce purchases at many website. The other potential source of fraud,

the production of 'white plastic' (counterfeit cards), can best be addressed by elimination of mag-stripe data as a nationwide initiative. Until then, the PIN remains the best means of averting use of stolen mag-stripe credentials at POS.

5. Optimal Configuration

To summarize, software-encryption PIN Debit can do everything the Fed needs to support secure, efficient and competitive debit card payments in the online venue—complementing and enhancing efforts to do the same thing in the physical world. The proposed attributes listed below constitute a configuration that will make PIN Debit successful:

-Familiar user interface: The floating PINpad is the clear consumer, merchant and bank favorite, and the option most likely to scale, and scale globally.
- Hosted system: Elimination of client software and downloads also fosters adoption and scaling, while ensuring that all access is gated through a known facility where the security can be monitored and upgraded for the benefit of all parties.
-Strong protection on user device: The floating PIN-pad and related user-security functionality all but eliminates keyboard sniffing and other device compromises, without making the user responsible for monitoring and invoking the security.
- Strong encryption: Software encryption has become much more powerful and efficient in the past decade, and is comprehensively more adoptable than the hardware alternative; Acculynk's security has been vetted by more than a dozen financial services networks and processors—attesting to its workability at banking standards of protection.
- Secure passing to EFT networks: A single, host-based interface ensures maximum security for network interconnectivity, as well as substantial efficiencies in maintaining and upgrading the connections—for the benefit of all parties.
- Compatibility with EFT formats and network conventions: A single host-based configuration also enables system-wide incorporation of updates and innovations in EFT formats and networking conventions.
- Ability to switch debit networks: As needed to assist in assuring greater debit card network competition, the host configuration can also act as a decision-maker for networks, banks and merchants to enable preferences for network routing; this could be a very effective 'virtual' stand-in while the rest of the banking infrastructure upgrades its physical capabilities along these lines.
- Global interoperability: A single host-based system is logically and physically transportable to other countries and their PIN-based debit networks and systems, facilitating global interoperability (and supporting the 5-year global debit card solution being worked on vis-à-vis ISO 20022).
- Inclusion in key standards bodies (e.g., EMV, PCI): The sooner the Fed (and/or other government entities) can 'decree' the viability of online PIN Debit, the sooner the key standards bodies can get started on doing their work (vis-à-vis some other relatively backward-oriented initiatives such as trying to get dynamic data authorization from mag-

stripe cards). This will minimize the waste in interim, transitional attempts at solving the problem, without picking winners and losers.

- Ability to virtualize/private-label/nationalize the host system: As a provider, Acculynk could certainly serve the entire industry as a 'utility' of sorts; but the design of the Acculynk host is modular and easily replicable for virtual or private-label instantiations, if market and competitive conditions dictate (provided that common security component remain consistently in-place and upgraded as necessary).
- Compensatory controls at banks to monitor phishing/unusual usage: This necessary and useful adjunct to the computing and communications security described by these attributes gets banks (and merchants) involved in understanding the risks inherent in remote environments *from both sides of a transaction*, and fosters individualized testing of different techniques that can add to and be shared by all parties.
- Software-encryption deployment: This deployment option is much less expensive and onerous than hardware options; PIN-equivalent options will incur much higher merchant acceptance hurdles (including payment timing); so moving the market to a veritable standard earlier rather than later will immensely useful for congealing market adoption and rationalizing investments (down the road, such standards can be generated by the appropriate standards bodies, such as ISO).
- Hardware token accommodation: Software-encryption of PINs can complement the marketplace's shift to chip generated tokens as a replacement and/protection for mag-stripe account credentials; while some commenters are critical of debit account PINS as 'static' identifiers, there is no better substitute for binding a consumer to a transaction.

Other Payments Systems Improvements with PIN.
A synchronized move to PIN Debit offline and online could help improve the U.S. payments system in several other important ways:

- *Better ROI for PIN adoption by merchants overall.* Reduced resistance by multi-channel merchants to upgrading their POS systems with PINpads/readers can be expected as the added value of having EFT payment interconnections for online (and mobile) use will increase the desire for a synonymous user experience and a better return-on-investment for moving to PIN acceptance overall. This could be of particular importance as merchants focus more on promoting more cost-effective debit card use in the wake of the Dodd-Frank reforms.
- *Huge savings could come from applying PINs to credit card use.* In the early-1990s,

MasterCard proposed transitioning to full PIN-based environment for both debit and credit cards—fostering a globally-compatible solution for securing signature-based card use across-the-board. With EMV Chip+PIN the concept of enabling both credit and debit for the same security-enhancing technology appears to be finally taking root in the U.S.; PIN is an indispensible part of that technology solution (indeed, evolution), and therefore an online solution is no longer an option.

- *PIN-authenticated ACH seems likely.* Fed officials have suggested in recent years that they might consider deploying the ACH as a default payment capability for any emerging payment system (e.g., digital goods/micropayments, electronic wallet offerings, etc.). It is fully electronic, well understood by most users, and reaches nearly all of the nation's banks securely and efficiently. It has been 'stress-tested' by NACHA on a number of new applications without undue challenges to the system—notably WEB (online) transactions. The biggest question would be how to protect the origination process for mobile transacting to ensure an adequate level of risk management and auditability. NACHA is currently testing mobile transactions through the WEB Standard Entry Class (SEC) code, but plans to create a new SEC (MOB?) as demand warrants. Adding a PIN to origination would solve most or all of this problem before it ever develops in mobile venues.
- *Second-factor authentication role can make Internet+mobile safer than any other venue.* Providing second factor authentication for other online/mobile-provider transactions is believed by many to be an ideal way to reduce fraud from other channels—incorporating a secure PIN for authentication rather than authorization/settlement. This function could be performed by a third-party host, or by Internet gateways, bank networks, issuer processors, and merchant processors.
- *Other applications for PIN security.* Securing healthcare, voting, vehicle registration, and other sensitive, confidential applications where user verification will facilitate and secure electronic processing and automation of paper-intensive processes would be another natural adjunct function an EFT-like PIN could perform (whether or not linked to any movement of funds, such as paying bills). So there is no real constraint, other than the inertia of the status quo, to making secure PIN use the common means of preserving confidentiality and security with a mechanism consumers embrace.

Conclusion

PIN Debit is clearly ready for prime-time online, and software-encryption solutions as demonstrated in the marketplace by Acculynk are eminently suitable for satisfying the Fed's Proposed Rulemaking objections—in particular fostering the PIN Debit option and business case for all transactional venues.

PIN Debit has proven to work effectively for online purchases and beyond with relatively little investment in infrastructure. In the software-encryption scenario, merchants merely need to install a payment API and check-out page 'bug' to enable host-verified PIN Debit transactions. Consumers merely need to enter in their 4- or 6-digit PINs via a 'floating PINpad' convention on their PC or mobile handset screen, much as they do today via an ATM. Research has shown that a floating PINpad convention was preferred by the vast proportion of consumers, merchants *and* issuers.

The business case for online transacting with PIN debit improves for all parties—including issuers, which save markedly on reduction of charge-backs and charge-offs from signature-debit card use. The value of Internet PIN Debit is substantive enough to warrant additional fees by merchants and even issuers, in return for the cost savings and improvement in efficiency.

As such, the next section addresses the specific comments solicited by the Fed for its proposed rulemakings, and includes specific actions the Fed should consider for removing the inertia of the status quo by encouraging adoption and use of the safest and most efficient payment option ever invented *online* as well as offline.

6. Federal Reserve Rulemaking

As outlined in the letter to Jennifer Johnson, Secretary Board of Governors of the Federal Reserve System, we believe that the PIN-debit online solution described in our "Comments" submission, and explained in detail this white paper offers constructive, readily implementable solutions for online debit card use that satisfies the spirit and intent of the four Rulemakings.

Interchange Rate Alternatives

The principal perspective we can offer is that use of PIN-debit online can dramatically reduce transactional fraud, charge-back costs and customer service activities—to the extent that use of PIN-debit online facilitates growth in new transaction volume and, over time, replaces signature-debit card use. This will enable issuers to have a better opportunity to reduce their debit card costs, and a better chance at making a profit—within the recommended cap on rates.

Fraud Adjustment

The Board requests comment on how to implement an adjustment to interchange fees for fraud-prevention costs. In particular, the Board is interested in commenters' input on the following questions:

1. Should the Board adopt technology-specific standards or non-prescriptive standards that an issuer must meet in order to be eligible to receive an adjustment to its interchange fee? What are the benefits and drawbacks of each approach? Are there other approaches to establishing the adjustment standards that the Board should consider?

In the case of online debit card use, there are three options that could be considered:

a) technology-specific standards;

b) non-prescriptive standards;

c) industry mandated standards.

Each option differs with regard to the likelihood and timing of market adoption as well as the consistency of security benefits offered. These variations are quite different for online debit usage in several important ways.

a. Technology specific standards
Technology-specific standards offer strong guidance, without an actual mandate, for

what forms of PIN-debit protection will be effective online, and therefore fairly compensated.
For online use, PINs can be included in the debit card transaction with three forms of protection:

i PIN-equivalent substitutes
ii. Hardware-encryption;
iii. Software-encryption;

i. The first option, PIN-equivalent or substitute alternatives cannot be viewed as sufficiently secure, and have not experienced consumer adoption. For example, one-time passwords, or pseudo-numbers, have been tried extensively over the past five years, but largely abandoned. The major hurdles were the tasks consumers had to perform to use them, and the difficulty using them in real-time and unfamiliarity of resolution when problems arose. Also they did not provide the consumer and merchant protections that true PIN-debit does.

The other two options--hardware and software encryption—utilize the PIN, and the EFT networks, directly; they have much more relevance as a sustainable solution for eCommerce, as discussed further in the accompanying white paper.

ii. Hardware-encrypting devices plugged into cardholder Internet devices can certainly perform the security required, but have several drawbacks such as cost of the devices, user difficulties with installation, aversion of users to additional equipment, potential operational issues, etc..

iii. Software-encryption methods are now every bit as secure, and when presented as a host-served PIN-input screen (e.g., with a floating PIN-pad interface that mimics the user ATM experience), require minimal change in behavior or deployment cost for issuers or consumers, and very modest costs for online merchants. Some investments are required by the EFT networks, but those are not considered to be substantial, and would be incurred in any deployment of online PIN verification for authorization.

Thus, a technology-specific standard that weighed the interests and investment/deployment requirements of all parties, *and* narrowed the choice of technology (e.g., software-encryption) at a sufficient standard of security (e.g.Triple-Data Encryption Standard,128 bit keys, as required for ATM and EFTPOS transactions) would suffice for providing a particular design configuration to the marketplace that

would still allow substantial variations in actual deployment options—in this case, the application of the software encryption algorithm.

b. Non-prescriptive standards
Allowing the marketplace to deploy PIN-debit online with non-prescriptive standards (e.g., any mechanism that performs 128-bit triple-DES conversion of the entered PIN at inception all the way through to the EFT network) would most likely perpetuate the extensive and mostly unproductive experimentation with deployment options and variations, without consistency in monitoring and auditing the security.

c. Industry mandated standards
The third option—an industry mandate (such as requiring *every* EFT network to offer software-encryption online PIN-debit within a certain time period, and perhaps a prescribed user interface for PIN-entry)—has the benefit of rationalizing total industry investment around a preferred solution that has consistent security and user interfaces and minimizes merchant confusion and acceptance costs. Clearly, this perhaps more determined posture might be viewed as running counter to the Fed's traditional restraint from endorsing specific solutions, but in the aftermath of the banking crisis, and in a post-Durbin environment, the need to minimize investment costs (and forestall continuing fraud losses) should be factored into its consideration.

Any such consideration should be viewed as transitional, rather than permanent, in any event. The progress of technology is relentless, and any industry standards developed and promulgated for the U.S. market should eventually flow into international standards ,e.g., ISO 20022, which has as an initial thrust standards for common debit card usage across borders. That will ensure new solutions that offer better protection and performance make their way into the payments marketplace.

2. If the Board adopts technology-specific standards, what technology or technologies should be required? What types of debit-card fraud would each technology be effective at substantially reducing? How should the Board assess the likely effectiveness of each fraud-prevention technology and its cost effectiveness? How could the standards be developed to encourage innovation in future technologies that are not specifically mentioned?

The preferred deployment—based on a decade of experience—for PIN-debit online is a technology that has the following principal components:

- 1) Protection of the PIN (and PAN) throughout entry and submission process via a secure host;

- 2) A natural, logical and secure user interface for PIN-entry;
- 3) Efficient merchant access to as many EFT networks and debit card accounts as possible;
- 4) Integration to as many EFT networks as possible from the secure hos
- 5) All provided in software that is easy to install and updatable across the system.

Once deployed, such technology will address both unfriendly and friendly fraud across-the-board, and will lead to substantial decreases in risk management and fraud reduction investments as the use of signature debit, card not present transactions declines over time.

The Fed can examine the relative risks and fraud reduction experience of PIN versus signature debit cards at the POS historically, and apply the same experience to online and mobile transaction venues. Metrics for both are now available, or can be obtained from either cooperating merchants (signature-debit versus signature-credit typically is only know by processors, and/or issuers, and they can be monitored over time and by merchant vertical.)

The Fed can also be instrumental in evaluating the preferred deployment with encryption algorithms, communications security, etc., then input these to trigger consideration and adoption by the various standards bodies in much the same way it does today. PIN-debit, which is based on the common and near-universal ISO 8583 format and its associated standards (and already is heavily examined and vetted for its 128-bit triple-DES for use at ATMs and via POS terminals) should translate easily to existing Internet standards and emerging mobile standards.

3. If the Board adopts non-prescriptive standards, how should they be set? What type of framework should be used to determine whether a fraud-prevention activity of an issuer is effective at reducing fraud and is cost-effective? Should the fraud-prevention activities that would be subject to reimbursement in the adjustment include activities that are not specific to debit-card transactions (or to card transactions more broadly)? For example, should know-your-customer due diligence performed at account opening be subject to reimbursement under the adjustment? If so, why? Are there industry-standard definitions for the types of fraud-prevention and data-security activities that could be reimbursed through the adjustment? How should the standard differ for signature- and PIN-based debit card programs?

Non-prescriptive standards for PIN-debit online would likely include hardware-encryption, software-encryption, and PIN-equivalent alternatives—fashioned to perform

largely identical functions, but likely with extensive variations in security. So the task of setting non-prescriptive standards would be difficult to derive, and it would not be certain how well they would work and scale, given the lack of high-volume/high-exposure experience.

Since issuers do relatively little in the way of online fraud management, and that is limited to signature-based cards, and further, that activity is more often than not outsourced to processors, where there is little differentiation between signature-debit and signature-credit, it is not clear that any fraud 'offset' makes sense for continued use of signature-debit.

PIN-debit online, as implemented by Acculynk, imposes no requirements on issuers, including no extra security requirements, but its adoption provides incremental benefit to the quest for fraud reduction overall for all. As an incentive for adoption, issuers should collect a fraud reduction 'offset' for deploying PIN-debit online. The mechanism in place of charging to merchants a merchant service fee that is comprised of interchange and acquirer mark-up provides a platform for enabling this value exchange between issuers and merchants

It does make sense to develop industry standards for debit card going forward, and there will be substantial differences for signature-debit versus PIN-debit. Given an even playing field for deployment, PIN-debit could be expected to continue to produce far less fraud than signature-debit, and has the added virtue that it can be instrumental in reducing so-called 'friendly fraud'. Industry estimates put the friendly fraud rate (where cardholders repudiate transactions that they actually know about but claim to be fraudulent and unauthorized) at 30-50% of today's online transactions. Similarly, a significant portion of online charge-backs occur for extraneous, and fraudulent, claims of non-receipt/non-delivery; issuer innovations in helping merchants eliminate this type of fraud would be welcome, too. Most importantly, issuer initiatives in reducing the number of charge-back 'recidivists'—across both signature-based and PIN-debit payments, in both online and offline venues—would be innovations worth rewarding.

4. Should the Board consider adopting an adjustment for fraud-prevention costs for only PIN-based debit card transactions, but not signature-based debit card transactions, at least for an initial adjustment, particularly given the lower incidence of fraud and lower chargeback rate for PIN-debit transactions? To what extent would an adjustment applied to only PIN-based debit card transactions (1) satisfy the criteria set forth in the statute for establishing issuer fraud-prevention standards, and (2) give appropriate weight to the factors for consideration set forth in the statute?

In general, the Fed should emphasize adoption and use of PIN-debit—online and offline and in any other venue—because of its superior consumer preference and performance, vis-à-vis signature-debit. Use of PIN-debit online means shifting the bulk of risk management and fraud prevention to the issuers, so if issuers are able to improve upon the inherent ability of this payment type to be more secure, they should be compensated for it.

5. Should the adjustment include only the costs of fraud-prevention activities that benefit merchants by, for example, reducing fraud losses that would be eligible for chargeback to the merchants? If not, why should merchants bear the cost of activities that do not directly benefit them? If the adjustment were limited in this manner, is there a risk that networks would change their rules to make more types of fraudulent transactions subject to chargeback?

Merchants should only pay for value they receive; if issuers' adoption of Internet PIN Debit leads to fraud mitigation and chargeback improvements , that is a great benefit to merchants and issuers. With respect to network rules governing treatment of fraud and classification of charge-backs, it is logical that guidelines be established and managed in a manner that prevents manipulation that results in any particular party being disadvantaged vis-à-vis the other party (e.g., policies that might encourage 'friendly fraud'). One possible manifestation of this new philosophy is to eliminate the Card Not Present (CNP) distinction that has characterized eCommerce for the past decade, and acknowledge that secure PIN entry and verification enable card use that is at least as strong as Card Present at POS (and in some respects offers stronger security).

6. To what extent, if at all, would issuers scale back their fraud-prevention and data-security activities if the cost of those activities were not reimbursed through an adjustment to the interchange fee?

Issuers should offer and support payment products that are secure and efficient; signature-debit clearly does not meet that criterion. However, if issuers are willing to take proactive steps, for the benefit of all stakeholders in the payment value chain, and invest in incremental fraud mitigation , a fraud adjustment makes good sense.

For example, part of implementing Chip+PIN is making the PIN available for every transaction in every venue; so while a fraud reduction 'offset' for implementing PIN-debit online is a logical inducement for issuers to deploy it, if such an incentive were not available, most issuers could be expected to still be motivated to deploy it for the 'good of the system', and to avoid operating at a cost disadvantage versus competitors.

A similar logic should work for merchants—even without some sort of financial inducement to adopt PIN-debit (or interchange 'surcharges' for delaying investment in Chip+PIN components, as occurs in some EMV deploying countries), merchants could be expected to deploy at least the PIN-entry and authentication component, since it would reduce their costs for debit card processing.

7. How should allowable costs that would be recovered through an adjustment be measured? Do covered issuers' cost accounting systems track costs at a sufficiently detailed level to determine the costs associated with individual fraud-prevention or data-security activities? How would the Board determine the allowable costs for prospective investments in major new technologies?

Issuer DDA systems tend to operate at a generic level for dozens of functions and modes of access, and usually combine fixed, semi-fixed and marginal costs together, spreading them across the entire line-of-business. This makes accounting for actual, incremental costs—as seen in the September Fed survey results—very difficult to measure. Guidance from the Fed (and other regulators) on how to improve the cost accounting for debit cards (and other banking products) would be enormously helpful for moving the industry to a more meaningful representation of their revenue, costs and profitability. Until that time, the Fed should avoid simply rebating or refunding part or all of issuer investments, and such investments should utilize new, standard metrics for returns on those investments. Thus, a holistic fraud mitigation and risk management 'system' needs to be created (perhaps embracing some of the best-practice accounting conventions of the most advanced banks and credit unions).

Such advances in accounting can and should be embraced by the core system provider outsourcers for most of the nation's smaller banks and credit unions—avoiding incremental costs of upgrading individual general ledger systems for more than 16,000 financial institutions. Perhaps a task force of industry accountants, consultants, auditors, core systems providers and other experts could be created and charged with doing this needed work. Such initiatives, for the 'good of the system' could easily be funded by temporary 'click' charges on transactions, collected from the merchants and allocated back to the issuers.

8. Should the Board adopt the same implementation approach for the adjustment that it adopts for the interchange fee standard, that is, either (1) an issuer-specific adjustment, with a safe harbor and cap, or (2) a cap?

9. How frequently should the Board review and update, if necessary, the adjustment standards?

A thorough assessment and benchmarking (which the Fed has begun with the surveys in September) conducted for a finite period of time (say, three years) would go a long way to providing a baseline for gauging industry performance. After this period, an annual audit would provide a basis for reviewing the effectiveness of industry's efforts against the always-growing

10. EFTA Section 920 requires that, in setting the adjustment for fraud-prevention costs and the standards that an issuer must meet to be eligible to receive the adjustment, the Board should consider the fraud-prevention and data-security costs of each party to the transaction and the cost of fraudulent transactions absorbed by each party to the transaction.

How should the Board factor these considerations into its rule? How can the Board effectively measure fraud-prevention and data-security costs of the 8 million merchants that accept debit cards in the United States?

Some of those 8 million merchants are clearly online (and more than million merchants are web-only). There, the great preponderance of fraud losses and risk management costs are borne by the merchants (76% according to the September survey). Ideally, banks, which have great knowledge about account use, behavior, and cardholder identity, should be incented to work with merchants, which have great knowledge about what happens in a transaction session. Unfortunately, the rules of Card Not Present (CNP) relegate the liability and responsibility to the merchants, and issuers effectively do not exert much effort and investment toward reducing risk at their end.

So, effective measurements would need to define what the issuer contributes to the process. Issuers might be incented to deploy and record results, and then begin to assemble best practices. In particular, it would be very valuable to incent and embrace efforts to work with merchant data to derive a more holistic risk management paradigm for both online and mobile transacting. If, as expected, PIN-debit performs substantially better than signature-debit, it might be constructive to encourage the industry to quit investing in trying to protect signature-debit, and channel its efforts and investment to ensuring that PIN-debit remains the safest payment system in any venue.

Network Exclusivity/Competition

A hosted system for PIN-debit online is purposely designed to interconnect with all EFT networks and all of their members and accounts; so creating a standard for PIN-debit use for Internet (and mobile) transactions naturally fosters a full selection of networks for consumers and merchants to choose from. In order for network competition to be

able to play out, debit cards need to carry at least one network that supports Internet PIN Debit. Otherwise, transactions will default to the signature network of record.

<$10 billion exemption

The complexities of ensuring all smaller financial institutions can participate at POS on an equal footing with banks and credit unions with greater than $10 billion in assets does not exist online for PIN-debit online. The host-system configuration (please see accompanying description), when connected to as many EFT networks (and cardholder accounts) as possible, provides a level playing field that lets the EFT network solution at the merchant website drive the transaction authorization and settlement to the card issuer—rather than being redirected by the merchant to some other issuer with perhaps a lower interchange. As well, the pricing model (used by Acculynk to-date) sets the price at a standard rate from the networks and the permitted rate by issuers, along with a negotiated rate from the merchants (which includes tiered pricing based on overall volume). Therefore, the structure for PIN-debit online has no mechanism for price discrimination, but can accommodate whatever the networks decide to charge—including proposals such as Visa's to support a bifurcated rate. Such pricing neutrality would not exist for signature-debit.

7. Conclusion

Collective research and experience have demonstrated that PIN Debit transacting is the most popular way to make payments for consumers and merchants alike, as well as providing a better solution for the banking industry than signature debit.

Internet PN Debit is the safest form of electronic payment offered and brings the benefits of PIN to the Web, namely a reduction in chargebacks and fraud that benefits all stakeholders across the payments value chain.

Among the different alternatives offered for bringing PIN Debit to the Internet – PIN equivalent options, hardware encryption and software encryption- a clear standard has emerged, Acculynk's PaySecure. This product has been developed and rolled out in the US to nine EFT networks, all major acquirers and thousands of Financial Institutions.

At this critical point in the rulemaking process the Fed is in a position to influence the adoption of this technology by:

- Issuing technology specific standards for Internet PIN Debit
- Allowing issuers to collect a fraud adjustment for implementing Internet PIN Debit
- Mandating Financial Institutions to carry at least one network that enables internet PIN Debit.

Appendix : Acculynk Profile

1. Brief History

In March 2009, Acculynk introduced the first software-only service for Internet PIN debit, PaySecure, in a pilot program that has grown to include top regional EFT networks and a number of significant merchants with commitments from some of the largest merchants in Ecommerce. This appendix outlines how the approach to market and simplicity of the PaySecure service has led to rapid and dramatic acceptance, positioning PaySecure as one of the most successful and significant enhancements to Internet payments in recent history.

PaySecure provides a simple user interface that utilizes a graphical PIN-pad for PIN entry and requires no consumer download, no hardware device, no enrollment and no redirection to use. Unlike alternative payment methods, consumers do not need to seek out PaySecure: the PIN-pad is simply presented as a payment option when a consumer's debit card can be used with a PIN and is in Acculynk's network of participating issuers.

In Acculynks first embodiment of IP, PaySecure was created to serve the financial services market. PaySecure can be utilized to "convert" signature debit transactions to PIN debit transactions. PaySecure can also be utilized to process PIN Only (ATM Only) debit cards. There are approximately 80 million PIN Only cards in issuance – none of which can be utilized online for eCommerce without Acculynk's PaySecure solution.

PaySecure is a software-only service that allows consumers to use their debit card with their bank-issued PIN to pay online, just they like they use their debit card at the retail point of sale today. Please see http://www.acculynk.com/payFirst/payFirst.html for a video of how PaySecure works.

2. Management Team and Board

Acculynk is backed by Oak Investment Partners with a total of $8.4BN capital committed to their companies and over 29 years experience in venture capital.

On the Board, there is broad industry representation:

Gene Lockhart – Former President and CEO, MasterCard
Rodman Reef – Retired Chairman and CEO, CitiShare, a Citigroup subsidiary
Stuart Harvey – CEO, Ceridien Corp
Ann Lamont – Managing Partner, Oak Investment Partners

Ashish Bahl – Chairman and CEO, Acculynk
Nandan Sheth – President and COO, Acculynk

The Management Team is comprised of industry veterans:
Ashish Bahl - Chairman and CEO. Prior experience includes Harbor Payments, American Express, IXL, Accenture
Nandan Sheth – President and COO. Prior experience includes Harbor Payments, American Express, Accenture.
Tim Barnett – CTO. Tim Barnett was previously the CTO of Elavon (Nova).
Ulrike Guigui – EVP. Prior experience includes MasterCard, GE Money and Citibank.

3. Patents

US Patent 6,209,104 - Issued

US patent 6,209,104 - Secure Data Entry and Visual Authentication System and Method is commonly referred to at Acculynk as the "Jalali" patent after the inventor. This patent is one of the key Acculynk patents.

The domain claimed under this is simple yet powerful. In this patent, a server generates a pseudo randomly arranged image (including icons associated with data), and transmits the image to a client for display (web page, smart phone, kiosk, etc…). A user selects at least one of the icons corresponding to desired input data. Location information for the selected icons is sent by the client to the server which compares that information to information and data in memory to ascertain the data input by the user.

US Patent 7,526,652 – Issued

US patent 7,526,652 - Secure PIN Management is the other core Acculynk patent.

The Jalali patent (above) allows Acculynk to acquire [X, Y] coordinate information. However, in order to turn the coordinates into an actual PIN value, an additional process is required. This is the functionality behind the Secure PIN Management patent.

US Patent 7,387,240 – Issued

US Patent 7,387,240 - System and Method of Secure Information Transfer is a patent issued to Acculynk's predecessor ATM Direct.

The patent embodies a process for downloading software securely to a terminal (PC, home computer, etc…), executing the software, and then transmitting data back to the original device.

US Patent Application 12/575,710 – Pending

Application 12/575,710 - Personalization Data Creation or Modification Systems and Methods is a patent which seeks protection for the Anti-Phishing capabilities that Acculynk built into the core PaySecure product.

The system initially permits a user to provide their email address before performing a PIN debit authorization using PaySecure. After (and only after) a successful PIN debit authentication, the user is sent an enrollment link to the email address provided prior to the purchase. Acculynk leverages the successful PIN authentication event to positively ID the user before permitting enrollment.

US Patent Application 61/331,163 – Pending

Application 61/331,163 - Financial Payment Systems and Methods for Obtaining Consumer Authorization of Overdraft Fees is a patent which seeks protection for a process to solicit consumers to enroll in overdraft protection with their Financial Institution.

The invention leverages the real-time nature of an eCommerce purchase to prompt the consumer to enroll in overdraft protection if the transaction is declined for Non-Sufficient Funds.

As outlined in this document, Accculynk has issued patents and intellectual property which allow it to operate exclusively in certain payment and security models. The nature of the patents is a natural fit for the Financial Services industry. The core patents provide the company a unique ability to handle very sensitive data in a secure yet intuitive manner.

The exclusivity afforded by the patents has numerous applications within payments but also within the greater security market in general. The patents can be leveraged in a mobile environment as well as online to create numerous offerings. Acculynk's initial application was to facilitate PIN debit processing in the online space – but the IP also allows the company to move into a much larger security-centric marketplace.

4. Security audits

PCI Status

Acculynk is audited yearly as a Level-1 Service Provider to the PCI standard. Acculynk first became PCI compliant in February of 2009. Acculynk continued compliance in 2010.

Acculynk's yearly audit is performed by TrustwaveThe 2011 compliance audit has been completed. Internal and External penetration testing is scheduled for completion by March of 2011. The Report on Compliance is currently in QA with Trustwave and will be submitted shortly to Visa and MasterCard. Acculynk will be one of the first companies in the US to comply with the new PCI DSS 2.0 standard.

TG3 Status

Acculynk is required to be assessed by a third party on a bi-annual basis for TG-3 compliance. Acculynk was assessed by Trustwave for TG-3 compliance in November of 2009. The results have been submitted by Trustwave to the appropriate EFT networks. Acculynk was found in compliance in all material respects.

SAS-70 Type I and II Status

Acculynk underwent both a SAS-70 type I and Type II audit in 2009. The audit was performed by Grant Thornton. In 2010 and beyond, only the type II assessment will be performed. Acculynks latest SAS-70 Type II was issued in November 2010.

5. Consumer testing

Prior to commercial introduction, Acculynk began testing consumer perception of PaySecure with a series of focus groups where consumers used the PaySecure beta and discussed their reaction to the product. The groups helped Acculynk understand initial consumer reaction and formulated the hypotheses for a larger, more intensive research study of 500 active[1] debit card users conducted by Javelin Strategy & Research in March 2009. Participants used PaySecure for a mock purchase and then answered a series of questions around the product's ease of use, perception of security, and intent to use PaySecure.

Acculynk's research efforts were the first to examine a consumer's willingness to enter their PIN online with an actual product. The research gave industry a glimpse into potential usage of PIN debit in the online environment. The study found that 80% of participants would use PaySecure when it was presented as a payment option by their trusted merchant. It also showed that consumers saw PaySecure as a more secure payment method, with 65% stating that they would feel safer buying on the Internet with PaySecure and that 48% would purchase more often on the Internet if they could use PaySecure. These early results indicated that consumers would accept PaySecure as a

[1] Active is defined as using a debit card at least 40% of the time online, and 40% of the time at the retail POS.

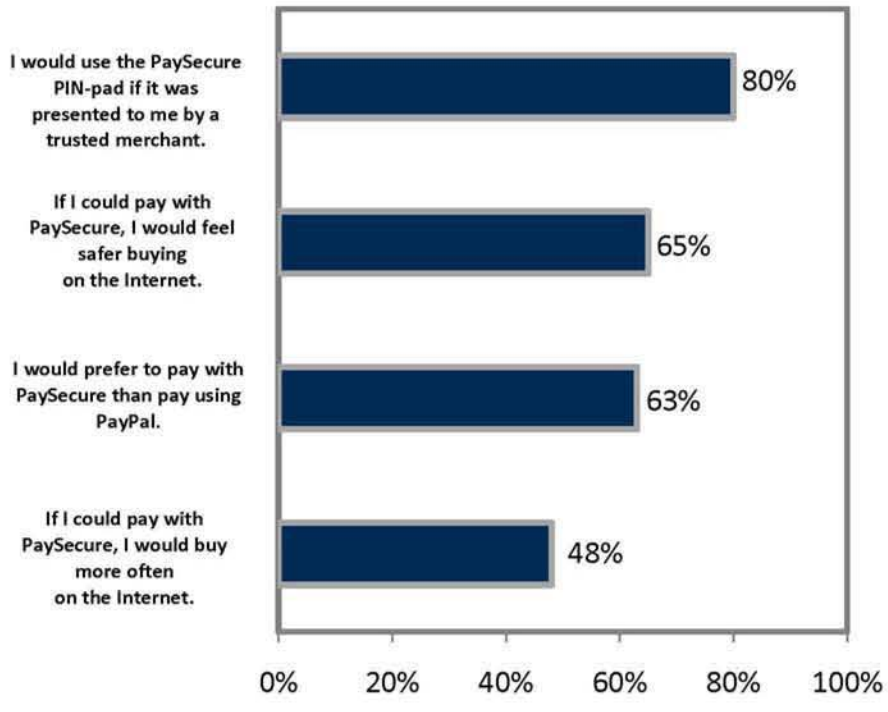
standard, online payment method, and that usage could actually increase trust in the Internet purchasing process and lead to additional sales.

PaySecure was designed to mimic the PIN entry process at the retail POS by giving consumers the choice to process their debit card transaction as a credit card by pressing Cancel on the PIN-pad, or continuing with PIN entry. In fact, 78% of consumers surveyed by Javelin agreed that the PaySecure PIN entry process was similar to and as simple as entering their PIN at the POS. The intuitive nature of the PaySecure payment process, consumers' familiarity with POS PIN debit and preference for PIN debit are lending to the impressive consumer usage of PaySecure to date.

Commercial results demonstrate that, when given the choice between processing their debit card transaction as credit or entering their PIN, approximately 1 out of every 2 consumers are choosing to use PaySecure.

- 55% of consumers that are presented PaySecure™ choose to use PIN debit and successfully complete PIN entry

This high level of usage, with minimal education and marketing, and no costly incentives, demonstrates that consumers understand the concept of using PIN debit online, and will use their PIN with PaySecure. And, as the Javelin study found, 79% of consumers surveyed would feel more secure using their debit card online with a PIN than using their debit card without a PIN. The low rate of cancellations on the PIN-pad also demonstrates that consumers are comfortable completing PIN entry with PaySecure – a testament to the usability of the product.



Once on the PIN-pad, consumers are completing PIN entry in an average of 30 seconds. Comparing these statistics to established alternative payment methods demonstrates that PaySecure has a clear value proposition to consumers in terms of a convenient, quick and simple payment process. Alternatives and card verification options, like Verified by Visa and MasterCard's SecureCode, first require that consumers enroll with the service before using. Depending on the consumer's speed, and the amount of information the payment service requires, this process could take anywhere from one minute to several minutes. When a consumer purchases with an alternative or verification service after enrollment, their checkout time could be lengthened by redirection to another website for payment, recollection of passwords/information, or even logging into their online banking account to complete the transaction.

The value proposition for the majority of alternatives and card verification services is security – few claim to be the most convenient payment method available. With PaySecure, consumers get an extra layer of security for their transaction in just a few seconds, using a PIN they already know, and pay right at the merchant checkout.

6. Acculynk Partners

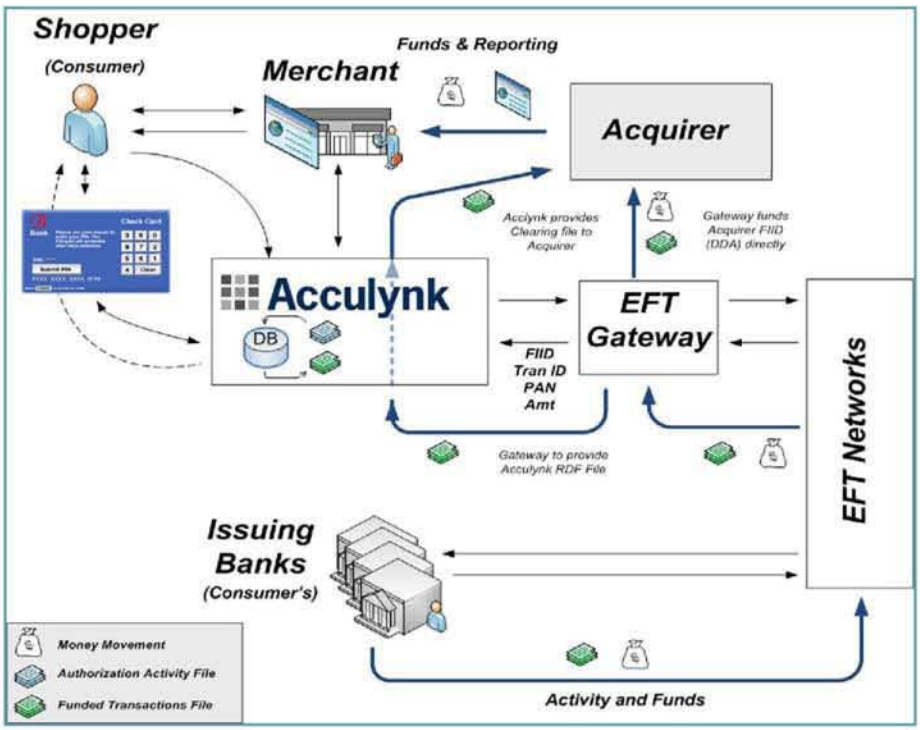
- PaySecure has become the standard for Internet PIN debit transactions as demonstrated by the rapid adoption of the payment method by merchants, EFT networks, bank issuers and payment processors:
    - **Merchants**: Over 3,000 active merchant storefronts are enabled with PaySecure today. Merchants include AirTran, Spirit Airlines, Sun Country Airlines, Ritz Interactive (Ritz Camera, Wolf Camera, etc.), ShoppersChoice, Jelly Belly Candy Company, and more. See a representative list at http://paysecure.acculynk.com/whereShop.php. Additionally, there are several big-box retailers and additional airlines that will go-live with PaySecure in 2011.
    - **EFT Networks**: Acculynk has partnerships with 9 EFT networks to process PaySecure transactions. These networks include ACCEL/Exchange, Alaska Option, Credit Union 24, the Jeanie Network, MasterCard (Maestro), NetWorks, NYCE, PULSE and SHAZAM.

- **Issuers**: We have over 6,000 issuers enabled across our live EFT networks.
- **Payment Processors**: Acculynk has partnerships with 6 payment processors, including:
  - Elavon (US Bank) – live
  - Merchant e-Solutions – live
  - JetPay – Q1 go-live
  - First Data Merchant Solutions (which includes their partners, such as Bank of America Merchant Services) – Q2 go-live
  - Chase Paymentech – Contracted
  - Heartland Payment Systems – Contracted

7. How it works--end-to-end

PaySecure works as follows:

1. Participating EFT networks provide their participating BIN's to Acculynk.
2. During the checkout process, the Merchant performs a checkbin query against these hosted BIN's.
3. If the BIN is found as participating, steps are followed to present the PIN Pad the consumer.
4. As the consumer selects his PIN with a mouse, the [X, Y] coordinates are captured (Jalali patent)
5. Acculynk "distills" or creates the PIN and builds an encrypted PIN Block (Secure PIN Management patent.)
6. The Merchant sends an authorization request to Acculynk.
7. Acculynk creates a POS Debit transaction and sends to the Issuing bank via the EFT networks for approval and returns the response to the Merchant



Acculynk authorizes PaySecure transactions across one of our 9 EFT networks to the issuing bank and returns the authorization to the merchant. At the end of the day, we provide a clearing file of PaySecure transactions to the merchant's acquirer; the acquirer reconciles the transactions and settles directly with the merchant – exactly how it is done today with a merchant's current systems. Because PaySecure is integrated directly into the acquirer's payment platform, there are no separate back-end connections, greatly minimizing the time and complexity for merchants that want to add PaySecure as a payment option.

With some simple integration, Merchants can take advantage of both signature debit conversion as well as PIN only processing of debit cards.