

BITS

FINANCIAL SERVICES
R O U N D T A B L E

ACCOUNT-TO-ACCOUNT SERVICES: EMERGING PRODUCT OVERVIEW

MARCH 2005

**A PUBLICATION OF THE BITS ACCOUNT-TO-ACCOUNT WORKING GROUP
PAYMENTS STRATEGIES STEERING COMMITTEE**

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
(202) 289-4322
WWW.BITSINFO.ORG

ACCOUNT-TO-ACCOUNT SERVICES: EMERGING PRODUCT OVERVIEW

TABLE OF CONTENTS

BITS ACCOUNT-TO-ACCOUNT WORKING GROUP	3
ABOUT BITS	4
EXECUTIVE SUMMARY	5
I. INTRODUCTION	6
II. TODAY’S A2A FUNCTIONALITY	7
A. Definition	7
B. How A2A Works.....	9
General Product Functionality: Current and Prospective	9
An Emerging Functionality	9
Stakeholders	10
A2A Service Offerings	11
Functionality from the FI/User’s Perspective	20
III. THE FUTURE OF A2A FUNCTIONALITY	21
A. A Nascent Technology: Opportunities for Growth.....	21
B. Levers	21
Interoperability.....	22
Role of Card Associations.....	22
Discrete, Credit-Only DDA Account Identifiers.....	22
C. Challenges.....	22
Cannibalization	22
Fraud Detection.....	22
APPENDIX: OPTIMUM TIME FOR STANDARDIZATION	24

THE BITS ACCOUNT-TO-ACCOUNT WORKING GROUP

Chair: Rodney Chard, Whitney Holding Corporation

Charter

The BITS Account-to-Account Working Group will examine the potential for financial institutions in A2A transfers, focusing on defining the functional and operational requirements for both online and batch processes. The Working Group was established under the auspices of the BITS Payments Strategies Steering Committee.

Objectives

- Evaluate and catalog existing and proposed functionality in all channels
- Identify gaps and overlaps in available services
- Explore potential benefits in a channel-independent approach
- Educate members on risks and advantages of account-to-account services

PARTICIPATING ORGANIZATIONS

BITS Member Companies

BB&T Corporation

Comerica Inc.

First National of Nebraska, Inc.

HSBC North America Holdings, Inc.

JPMorgan Chase & Co.

SunTrust Banks, Inc.

Synovus

The Bank of New York Company, Inc.

Wachovia Corporation

Wells Fargo & Company

Whitney Holding Corporation

BITS Affiliate Members

Independent Community Bankers of America

NACHA

Participating Networks

STAR

NYCE

The Clearing House

Participating Service Providers

Online Resources

CashEdge

ABOUT BITS

BITS is a nonprofit industry consortium whose members are 100 of the largest financial institutions in the United States. BITS was formed by the CEOs of these institutions to serve as the strategic “brain trust” to provide intellectual capital and address emerging issues where financial services, technology and commerce intersect, acting quickly to address problems and galvanize the industry. BITS’ activities are driven by the CEOs and their appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee and BITS Advisory Council. These leaders identify issues, develop strategic recommendations and implement the CEOs’ decisions. BITS also facilitates cooperation between the financial services industry and other sectors of the nation’s critical infrastructure, government organizations, technology providers and third-party service providers.

BITS’ mandate is to:

- Facilitate the growth of electronic banking and financial services
- Facilitate development of superior, market-driven technologies
- Maintain the industry’s role at the heart of the payments system as e-commerce evolves
- Sustain consumer confidence and trust by ensuring the safety, soundness, privacy and security of financial transactions
- Leverage resources and infrastructure across the industry

For more information about BITS, go to www.bitsinfo.org.

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON DC 20004
(202) 289-4322

EXECUTIVE SUMMARY

Account-to-account (A2A) electronic funds transfers enable consumer-directed funds flow between consumer accounts. These accounts may be those of an individual consumer located at different financial institutions (FIs), or of different customers within or outside of a single financial institution. Financial institutions are increasingly entering the A2A business. Although still nascent, A2A services are growing in size and complexity.

The BITS Account-to-Account Working Group developed this paper to understand the opportunities and risks inherent in this latest adjunct to online banking and help BITS members make the most of an emerging and dynamic financial tool.

This paper provides an overview of A2A services including:

- Stakeholders: FIs, third party service providers and networks;
- Current markets for A2A products;
- Mechanics of A2A functionality;
- Security features;
- Risk-mitigation tools;
- Factors impeding growth;
- Areas of opportunity; and
- Customer benefits.

The paper further explores the processes, rules and standards that currently define A2A functionality and the tools at our disposal to help shape its future.

I. INTRODUCTION

Financial institutions (FIs) are increasingly entering the Account-to-Account (A2A) business.¹ In 2004, leading U.S. FIs launched A2A services in a variety of forms, offering a range of functionality from the transfer of funds among a customer's accounts within a single institution to transfers across institutions and across borders.

Although still nascent, A2A services are growing in size and complexity. According to Celent Communications, 14 percent of institutions polled offered A2A services and nearly half of those that did not offer A2A services were considering adding them in the next 12 months.² Aite Group provides the following growth estimates for Web-initiated EFT/ACH consumer transfers in the U.S. (values in billions).³

2003	2004	2005	2006	2007	2008
\$5.34	\$11.19	\$15.20	\$21.14	\$31.05	\$44.85
	109%	36%	39%	47%	44%

A2A growth is the result of increasing consumer comfort with online banking products, greater availability of FI-offered A2A products and overall projections for increased Internet use. From the consumer's perspective, A2A offers lower cost compared to existing remittance products, increased convenience and "one-stop" financial shopping from a trusted provider. Since nearly a quarter of all checks written are consumer-to-consumer transactions, under the right circumstances A2A's potential is sizeable.

New technologies allow FIs to offer convenient, timely and secure access to funds transfer services. The BITS A2A Working Group's goals are to understand the opportunities and risks inherent in this latest adjunct to online banking and help BITS members make the most of an emerging and dynamic financial tool.

This paper provides an overview of A2A services including:

- Stakeholders: FIs, third party service providers and networks;
- Current markets for A2A products;
- Mechanics of A2A functionality;
- Security features;
- Risk-mitigation tools;
- Factors impeding growth;
- Areas of opportunity; and
- Customer benefits.

With respect to stakeholders, this paper incorporates the perspectives of current active players. However, the field of competitors is expected to broaden with active competition among FI and non-FI players.

¹ A2A electronic funds transfers enable consumer-directed funds flow between consumer accounts. These accounts may be those of an individual consumer located at different financial institutions, or of different customers within or outside of a single financial institution. Transfers among customers are also referred to as person-to-person (P2P) transactions.

² Celent Communications, 2004.

³ Aite Group, March 2005. Estimates include Web-initiated consumer transfers over ACH/EFT networks to fund new checking and savings accounts or to make transfers between existing accounts at different institutions and excludes transfers made via EBPP, PayPal, and intra-bank transfers ("on-us A2A").

The BITS A2A Working Group examined current offerings and identified several aspects of A2A functionality that warrant further exploration, or that could benefit from additional cross-industry review and development. For example:

- The majority of today’s A2A transactions are ACH based. While the potential for widespread adoption lies in a real-time functionality, current EFT network switching capability is limited by the lack of gateway agreements among the major regional EFT systems and the fact that the two national credit card companies do not presently offer a domestic A2A service through their own real-time capacity. Ubiquitous real-time access is important to the growth of a robust domestic A2A service. FIs interested in improving the reach and robustness of A2A services should work with their network partners on broadening each channel’s footprint by establishing a gateway service or, in the case of the credit card companies, establishing a basic A2A footprint in the U.S. (Both Visa and MasterCard offer such products on a cross-border basis within the EU.)
- The ISO 8583 standard is the basis for most real-time EFT network switching and, as A2A functionality has developed, networks have used proprietary extensions for this specific functionality. Establishing a single, ISO-endorsed set of extensions for use across networks would improve interoperability and efficiency.
- The security of A2A transfers is sometimes supported by surrogate account identifiers that mask an end user’s DDA account number.⁴ The Clearing House has developed (originally for use outside of the A2A space) a Universal Payments Identification Code (UPIC) for credit-only use in the ACH. The STAR and NYCE networks rely on the personal account number (PAN) to mask the DDA and allow for a second, credit-only PAN at the issuer’s option. To maximize efficiency and enhance safety and soundness, the industry could consider a single, credit-only account surrogate that functions across all channels.
- Compliance with key regulations—such as the Office of Foreign Assets Control (OFAC), the USA Patriot Act and the Bank Secrecy Act—is a significant concern. As the volume of A2A transfers rise, so too do risks of money laundering and other fraud events. Risk also rises with the number of discrete paths over which A2A transactions may be routed, and FIs must have the ability to analyze both inbound and outbound transactions across all channels seamlessly. **While cross-channel management of FI services has been promoted across the industry for several years, the majority of institutions have yet to achieve a holistic view of their payments business.** Given the absence of a seamless management approach, FIs need to maintain or adopt rigorous analysis of money movement, regardless of type or channel of initiation.
- Analysis of A2A transfers needs to be categorized by method of authentication. The BITS A2A Working Group has coordinated with the BITS Fraud Reduction Steering Committee to share FI experiences and develop best practices to mitigate A2A related fraud.

The following sections explore the processes, rules and standards that currently define A2A functionality and the tools at our disposal to help shape its future.

II. TODAY’S A2A FUNCTIONALITY

A. Definition

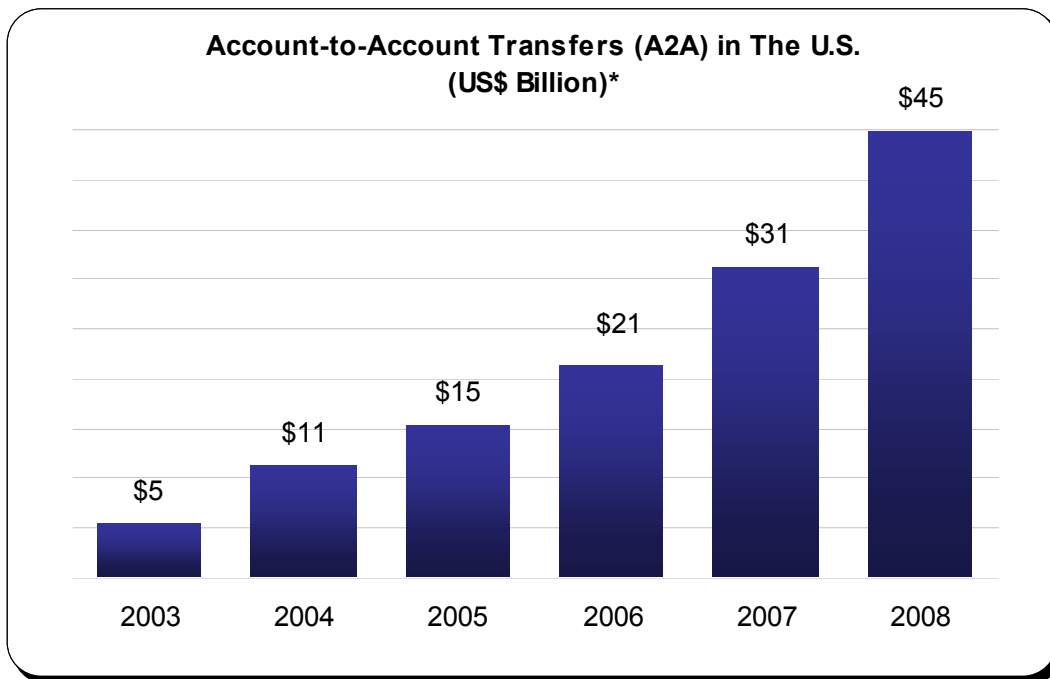
The term “A2A services” may refer to the transfer of funds between a single consumer’s accounts within or across FIs (“me-to-me” transfers) or more broadly to the transfer of funds from any account to any account within or across institutions (“me-to-you” transfers). CashEdge estimates the average me-to-me transaction at \$1,000, while TowerGroup data find the average person-to-person (P2P) payment is \$47.

⁴ Although the DDA is referenced throughout this paper as the source account for A2A transfers, A2A can and in some cases is used for transfers to and from other types of accounts, such as brokerage accounts (CMA).

Although BITS defines A2A in its broadest sense (incorporating both “me-to-me” and “me-to-you” transactions), with a few significant exceptions in the U.S., the functionality has been limited in geographic scope to transfers between U.S.-based accounts.

From a U.S. perspective, A2A services are just beginning to include international transfer capability. At least one large, international FI incorporated in the U.S. provides an in-house, cross-border service with transactions flowing to and from twelve countries. This functionality is, however, limited in reach to accounts housed within the firm’s international branch network and the range of U.S.-registered DDAs. OFAC restricts transfers to those stemming from and flowing to DDAs registered in the U.S. Similar transfers between, from or to a non-U.S. account could not be performed. Although OFAC has not published an official evaluation of this scenario, it has indicated that both sending and receiving accounts must be U.S. registered. Clarification from OFAC on these restrictions is needed before cross-border transfers proliferate, except among the largest international banking institutions.

Domestically and internationally, A2A transfers represent the cusp of a new stage of development, with significant industry potential for network providers, third-party processors and FIs.

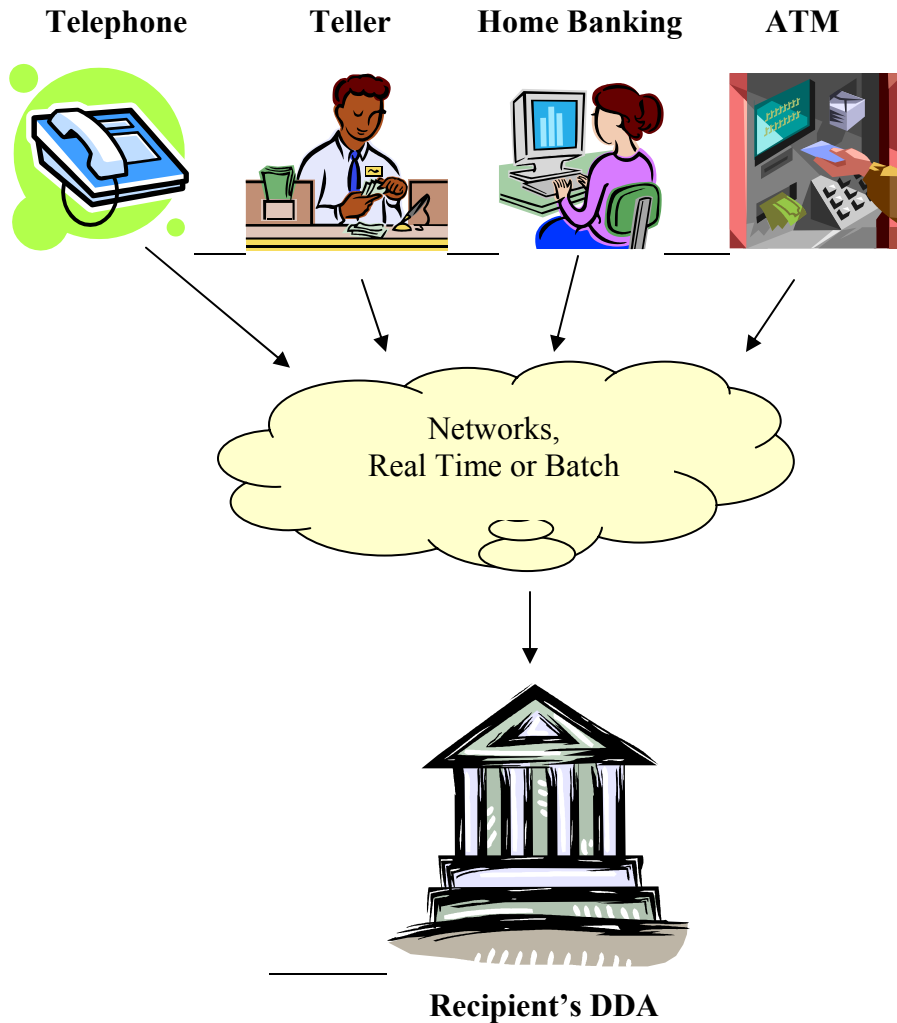


Source: Aite Group, March 2005. Estimates include Web-initiated consumer transfers over ACH/EFT networks to fund new checking and savings accounts or make transfers between existing accounts at different institutions and exclude transfers made via EBPP, PayPal, and intra-bank transfers (“on-us A2A”). Projections depend in part on how the industry manages the challenges and choices inherent in this evolving product.

B. How A2A Works

General Product Functionality: Current and Prospective

A2A services provide additional DDA functionality to the FI and its customers. The chart below illustrates the links among access channels, the DDA and the networks that support A2A transfers.



An Emerging Functionality

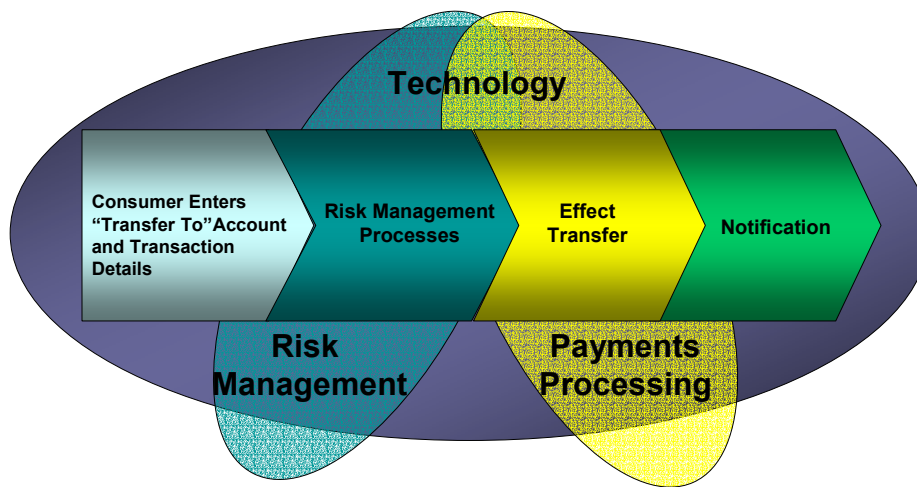
A2A functionality is proliferating rapidly. In the second quarter of 2004, Online Resources reported 80 active FIs offering A2A accounts, and as of March 2005 that number exceeded 130. Growth of A2A is equally significant at CashEdge, where more than 200 FIs offer A2A services.⁵ The largest FIs are more likely to offer A2A services although the product is showing signs of moving down market.

⁵ Online Resources provides services CashEdge. CashEdge data reflect those services.

A2A services can be provided by third parties, as in the PayPal model, or by FIs using existing industry infrastructure. A2A products may be offered as a standalone or integrated with an FI's e-banking application. At this time, only large FIs are offering A2A in this way. This paper illustrates how FI-based offerings bring together the technology offered by a third party service provider with the online bank services of an FI to transfer funds among consumer accounts through the FI's existing network relationships (e.g., batch ACH and real-time EFT networks).

The graphic below illustrates the interplay of technology with risk management and payment processing services that takes place as a transfer flows from initiation to completion and notification.

Typical Process Flow for A2A Transfers



Source: TowerGroup

Stakeholders

Three primary types of organizations work together to provide A2A services:

- **Financial Service Providers.** FIs are beginning to provide customers with access to A2A transfers as an adjunct to existing banking services. Access is primarily but not uniformly tied to online banking and A2A is often an adjunct to e-billing and payment products. Significantly, several large FIs have already announced A2A service expansions.

Initial service options vary widely in scope. The most basic service allows customers to transfer funds from one account to another within the same institution. Others offer transfers within a single customer's accounts across institutions. More sophisticated products allow inter-FI transfers from customer to customer. Bank-to-brokerage transfers are offered by some institutions, as are international transfers for accounts within the same institution.

- **Third Party Service Providers.** While FIs may interface directly with the networks that provide A2A transfer, more frequently a third party technology firm contracts with the FI to provide a

seamless, white-label product, which the FI offers to customers under its own brand. A primary service provider may outsource aspects of the service to other third-party technology firms or may provide services in conjunction with these third parties to the FI. Transactions are executed by the provider via the FI's network relationship. By contract, the third party acts as an extension of the FI, and the FI retains the customer relationship along with the related liabilities and risks.

Third party service providers in turn may outsource applications to a range of technology firms for specific applications. A subset of FIs, including several of the largest organizations, provides A2A services in-house without a third party service provider. However, outsourcing predominates in the current market with most services provided by third-party service providers.

- **EFT Networks.** The electronic funds transfer networks (STAR, NYCE, EPN, the Federal Reserve *et al*) provide inter-bank connectivity, i.e., the rails on which inter-bank A2A transfers ride. These network services are evolving but currently function on parallel, non-intersecting paths. Service varies in functionality and reach, the latter primarily reflecting the current lack of interoperability across real-time EFT providers. Going forward, interoperability between real-time EFT switching systems may be achieved. Both networks have indicated that policy—not infrastructure—is what prevents cross-channel transfers today. Sufficient requests for change among network members could result in an open system. However, the timing for such a shift is difficult to forecast.

A2A Service Offerings

A wide range of A2A service offerings is available today and more are coming. Variations exist in the type and amount of information required to execute a transfer, in applicable costs (based primarily on requested speed of delivery), available delivery times and authorization and authentication procedures.

The amount of information required of the sender and provided to the receiver is determined in part by Regulation E in the ACH and EFT network environments. The EFT networks vary somewhat in the content and format of the information provided by the sending institution. STAR, for example, always provides the sending institution's name, while NYCE provides an option for the sending FI to request cardholder name information, which is then passed through to the receiving FI. Both networks, however, provide institutional identifiers (e.g., PAN, transaction identifier) and all information needed to comply with relevant regulations such as Regulation E, OFAC, the USA Patriot Act, and the Bank Secrecy Act (including the Travel Rule).⁶ Vetting of other compliance regulations and laws has also been reviewed (e.g., privacy, EFT laws, and Customer Information Guidelines). In STAR's case, outside counsel provided input on the level of information the network must provide to the sending and receiving FI in order to comply with regulations. Advice included an interpretation of Regulation E that requires the receiving FI to include the sending customer's name in the statement description. Dollar limits also must be placed on the transactions, a task that the network usually leaves to the individual FI. This stipulation is intended to help FIs stay within strict requirements for reporting large transfers and to deflect money-laundering attempts.

Delivery speeds depend in part on the conduit or rail selected for the transfer. For example:

- ACH transactions settle on a daily basis one or two days later. However, some providers offer a “good funds” processing model and assume the return risk inherent in providing funds in advance of clearing and settlement.
- ATM/EFT network-based options offer real-time availability (as opposed to real-time movement capabilities). Actual net settlement is bundled into a network's regular settlement process, typically via

⁶ The Bank Secrecy Act Rule [31CFR 1-3.33 (g)], also referred to as the “Travel Rule,” requires all FIs to pass certain information to the next FI in certain funds transmittals involving more than one institution. (U.S. Department of the Treasury FinCen Advisory, January 1997.)

ACH on the morning of the following business day. EFT rules of engagement guarantee receipt of funds to the receiving FI, which means that real-time movement is less important than the “good funds” guarantee and real-time availability.

In addition to consumer-facing distinctions, offerings also differ in terms of fraud applications and other internal security procedures implemented by the service provider and/or the FI. More information on the security and fraud detection features in place with each stakeholder’s service is provided below.

Prospects for Growth

A2A services are often promoted as part of an overall package of online consumer banking products in conjunction with bill pay and aggregation options. As an adjunct to account aggregation, A2A could provide the lynchpin that successfully consolidates the customer’s view of his or her account holdings across FIs. However, A2A falls short of providing a convenient trigger with which to transfer funds from account to account for optimization purposes. By combining aggregation with A2A services, the customer can more easily manage and optimize account holdings by analyzing overall portfolio composition and moving funds into and out of selected accounts.

The considerable success of the PayPal model contributes to analysts’ positive expectations for A2A growth. With 15.5 million customers conducting transactions in 2Q04, PayPal is the dominant tool for P2P auction payments and has a growing non-auction related product line.⁷ PayPal enables both DDA and credit card-based funds movement into a consumer’s account. (A2A facilitates primarily DDA-based transfers, though brokerage accounts are tapped in some instances.) Consumers currently use A2A for one-time and repeat transactions, primarily among family members and well-known contacts. Today, the majority of A2A transfers are among known parties. Comfort with Internet transactions between a range of parties, with varying levels of assumed trust among sender and receiver, will contribute to A2A’s success.

As the service matures, A2A transfers will increasingly be launched from all DDA electronic access devices (ATM, Internet, telephone/VRU, etc.). Existing services can support these options today; the choice lies with the FI to activate them.

A2A from the FI’s Perspective

The following steps describe a generic A2A service from the FI’s perspective:

- The FI optionally enables A2A sender functionality directly to ACH, NYCE or STAR network, or via a third party entity. For instance, using proprietary or third party applications (such as Corillian, Digital Insight, or Certegy), the FI may connect with a transfer service provider (such as CashEdge or Online Resources).
- When the third party provides the online transfer service, this application integrates seamlessly with the FI’s home banking software and allows for an FI-branded customer interface.
- The network carries the transaction from the sending FI to the receiving FI.
- If authentication is approved for the sending and receiving accounts, the respective funds transfer (credit) is posted to the receiving account.
- Funds availability typically occurs in real time if the transaction clears through NYCE and STAR. Third party applications also offer options ranging from real-time to batch one- or two-day settlement.

⁷ *American Banker*, “PayPal Accounts Blocked As an Update Goes Awry,” Daniel Wolfe (October 13, 2004).

Today, real-time transactions must flow through a single network; although multiple EFT networks are active in A2A, there is no gateway service or inter-network switch currently available from an EFT network. If the demand for gateway switching of A2A transactions increases, networks may provide the service. Alternatively, MasterCard and Visa may offer a domestic A2A service as they do today in the EU.

A 2001 Dove Consulting study⁸ found that speed of transfer is among the top features sought by consumers in an A2A product. Speed to access was the second most important feature, second only to—and related to—cost. Currently, only two EFT networks offer a real-time transfer service.

Early adopters of A2A are more likely to be Internet savvy. Research and early experience suggest age also plays a role in adoption, with younger consumers comprising a larger share of users, particularly online—a fact that bodes well for growth.

Among the advantages to the FI, A2A transfer services:

- Tap into a strong growth market of online payments.
- Aid asset gathering. More funds flow into rather than out of the offering FI's DDA. One major FI found that in 2004, 75 percent of transfers were, on average, inbound.⁹
- Offer a competitive advantage (among FIs and third-party money transfer providers).
- Enhance the utility of online financial services (encourages “one-stop” banking).
- Reduce disintermediation risk by keeping consumer money transfer business in-house.
- Leverage existing rails.
- Further reduce reliance on paper checks.
- Primarily take volume away from the paper check, thereby expediting the industry’s push toward electrification.
- Generally require only a moderate investment to establish, assuming risk-monitoring systems are properly configured.
- Create a new revenue source, which may become significant in the long term.
- Provide interchange opportunities to the receiving FI.
- Improve account/customer retention.
- Offer a range of implementation options (in-house or third-party sourced).
- Can be customized and branded.

Challenges

- **Interoperability.** Limitations on network connectivity currently limit product reach.¹⁰ Providing flexible services with options for speed and broad access will enhance adoption. Flexible standards are also key to interoperability; ISO 8583 is universally applied in real-time A2A transfers but with unique, network specific extensions. The financial services industry would benefit from a uniform set of ISO 8583 extensions before more actors, such as the major card associations, become active in this space domestically. (The timing for such an effort to create universal A2A extensions fits well with the timeline for product adoption.)

A2A services are at the point in development at which converged standards could best foster greater interoperability among service providers. See the Appendix for an illustration of this point.

⁸ This private and confidential study was commissioned by a major EFT network.

⁹ *American Banker*, “A Person-to-Person Offshoot is Putting Up Good Numbers,” Daniel Wolfe (February 25, 2004).

¹⁰ That is, the lack of gateway functionality that enables a transaction that starts on one network to switch to and end on another.

- **Security.** A2A security is a primary concern to FIs and users of A2A. FIs bear the fiduciary responsibility and liability for transactions flowing through their institutions and A2A has the potential to significantly increase the volume and rate of transactions passing through customer accounts. A2A customer authentication methods will vary as a function of the network and initiation device used to enable the transaction. No matter what combination of network and initiation devices a customer uses for A2A, good authentication procedures are critical. Transfer speeds will continue to accelerate as offerings expand beyond the ACH's one- or two-day settlement capabilities.¹¹ Combined increases in speed and volume warrant increased monitoring for fraud, particularly related to money laundering and compliance with related regulations such as OFAC, the USA Patriot Act and the Bank Secrecy Act.

The Dove Consulting survey found that consumers strongly preferred FI-branded services, which they viewed as more likely to provide relatively stronger security. The prevalence of phishing and concerns about viruses, spyware and identity theft contribute to the challenge of advancing online services and maintaining or improving consumer confidence. Security is even more of an issue for consumers with less experience and comfort with electronic transactions. An FI's ability to enable consumer confidence in its security measures is central to the success of its online products. Ensuring that FIs fully understand the safety and soundness considerations that relate to emerging A2A functionality is key to promoting overall adoption.

How do FIs view A2A security in general? Is it robust enough? FIs are generally satisfied with identification procedures for the sender, which include online banking passwords, ATM PINs, etc. The challenge is how to identify the receiver. Rules and procedures for wire transfer could be adopted or used as a guideline for authentication procedures in the A2A space. New procedures may be needed to accommodate new processes such as the UPIC and pseudo-PAN identifiers (which work only for credit transfers); however, wire transfer guidelines could be used as well.

Service providers' key challenges concern the technical competencies required to upgrade or enhance current hardware and/or software. ATMs generally need to be of a certain series to be eligible for upgrade to terminal-driving software. Metavante, for example, has performed such upgrades for NCR and Diebold platforms; Fujitsu is expected to do the same in the future. For e-banking, the barrier is in connecting authorization capability to the host platform (posting real-time debit and simultaneously sending credit outward to the destination FI).

For the network: Any network transactions initiated online require the processor to complete an Internet compliance audit, for which the networks have a list of Internet-specific requirements. The absence of a standard Internet authentication method has prevented networks from allowing a cardholder to initiate an inter-bank transfer debit. An Internet authentication method would also solve the problem of validating the receiver's identity.

- **Fraud Prevention.** Fraud prevention stands shoulder to shoulder with security in evaluating A2A services. Moreover, fraud risks cannot be addressed in a vacuum. A coordinated approach, beginning with an evaluation of risks as they are managed by each stakeholder, is needed to foster an environment conducive to promoting adoption.

Ultimately, FIs are responsible for risk mitigation and hold all liability for their customer's funds. The service provider can take on risk mitigation if it is covered by a service contract, but the payment networks will hold the sending FI liable for most issues. STAR's rules, for example, outline the

¹¹ There are a number of scenarios, some of which can take one to two days as stated. However, many cases take three or more days, for example in the case of a "pull" from an external bank or when a service provider is in the middle of the transaction (with a third bank).

sending FI's responsibilities and make stipulations that protect the recipient. These rules cover systems security, truncation of the recipient PAN, etc.

NYCE requires the sending and receiving FI to perform as instructed by the acquirer. Otherwise, the breaching party is held responsible. A2A transactions are generally final when sent. Once a transaction is made, the receiving FI extends goodwill to the sending FI to make any changes that might be necessary (such as if the sending cardholder declares an unauthorized use of his card for A2A). FI technical and business policy measures limit abuse and carelessness.

The BITS Fraud Reduction Steering Committee recommends that FIs track fraud losses first by channel and then by transaction type (e.g., A2A). If patterns of fraud arise across channels and transaction types, FIs should build in loss reporting capabilities in a manner that specifically identifies the transactions causing the increase, such as a matrix report that identifies channels, transaction types and initiation device types (phone, Web, ATM, branch, etc.).

Another key aspect of fraud management in this space is to ensure the best available settlement timeframes and that rejected transactions happen immediately or are proactively identified prior to crediting accounts. Rejected transactions identified after the fact require timely investigative processes and sound procedures for monitoring and managing errors and losses. Standard procedures should include identifying all potential scenarios that could produce a rejection and capturing and including this data in ongoing fraud monitoring databases. The ability to establish rules in advance that are based on known behavior patterns will help capture exceptions in a real-time environment and are essential in developing a strong, proactive fraud reduction program.

- **Money Laundering.** This is another area of concern to FIs involved in or increasing their presence in the money transfer business. A number of existing laws and regulations need to be addressed, including the USA Patriot Act and the Bank Secrecy Act (BSA). FIs providing A2A services need to assure careful compliance with BSA regulations and develop systems that can produce an adequate level of transparency for reporting purposes. One overriding issue is clear: FIs involved in or becoming involved in A2A need to be alert to changes in federal money laundering mandates and the ways existing mandates are applied. This requires a team approach at each FI to appropriately monitor and manage risk. **While liability is concentrated on the sender, both sending and receiving FIs will likely be accountable for establishing key controls and monitoring transactions to identify irregular activity.** Continued legal expertise is required for ongoing due diligence. Industry wide, cooperation is needed to adapt security and fraud prevention techniques to mitigate risks associated with potentially high-volume, high-speed transactions, and to help FIs conform to more stringent regulations

While safety and soundness are the overriding concerns for an institution in managing fraud and money laundering issues, regulatory compliance is also a major and growing concern. As noted above, FIs must follow a growing set of laws and regulations. As the volume of A2A transactions grows, FIs are working to ensure that systems, procedures and personnel are in place to adequately review and coordinate the monitoring process so that increased A2A activity does not translate into additional fraud and security issues. Again, success requires a cross-enterprise, cooperative approach.

- **Risk Management.** In managing risk, FIs should understand the full scope of their liability in A2A transactions. The sender assures compliance with internal and external (network and regulatory) dollar limits.¹² FIs may contract with other parties for various services but are legally responsible for the transactions processed on their behalf.

¹² Single transactions and aggregate over time.

Appropriate due diligence in outsourced processes is important to safety and soundness, as lack of appropriate measures could considerably increase risk and threaten product adoption.¹³ The applicable payment network rules address this point; STAR, for example, assigns liability to the sending FI. The network's automated exception processing tool offers a means of allowing the sending and receiving FI to reverse a chargeback, assuming that agreement between the institutions is reached.¹⁴

There are exceptions to the rule of assigning liability to the sending FI. For example, on the NYCE network where Bank A is the sender and Bank B the receiver, a third institution, Bank C, can acquire a transfer via one of its ATM platforms. In this case, if the acquiring FI makes an operational error, the responsibility is theirs. The acquirer is accountable to perform exactly as the cardholder instructs. In such an instance, the originating funds FI is responsible for submitting a query to NYCE for subsequent communication to the destination FI.

As with wire transfers, A2A funds movement is designed to be final: funds are sent and the transaction is complete. The originating FI reserves the right to petition the destination FI if funds were sent to the wrong account or if an incorrect amount was delivered. More typically, the sender will initiate transactions from his or her own FI (from Bank A not Bank C) via ATM or e-banking, in which case liability is consistent with non-A2A transactions.

Risks and Mitigants

Below is a list of the primary risks associated with A2A transfers along with corresponding mitigants. Not all mitigants are uniformly applied and FIs considering A2A services should explore available options.

FIs generally want to use the same restrictions with A2A as they have with wire and check transactions. However, transaction and dollar limits could substitute for more stringent restrictions on checks and wires. According to the BITS Fraud Reduction Steering Committee, A2A requires more timely fraud detection. **FIs must be able to monitor cross-channel risks, and the majority of FIs are still establishing or refining this process.**

- **Account Authorization Risk.** This risk exists when the account is otherwise not valid, or when access is not authorized, for example with spousal fraud. These risks can be mitigated by a range of mechanisms to validate external account ownership and real-time risk management algorithms.

According to CashEdge, account authorization risk must be monitored continuously. When each account is set up, ownership is validated using a variety of methods: checking against commercial check printer databases, checking the online banking website, etc. Some FIs are considering adding pseudo PANs to their authorization risk arsenal to prevent unauthorized debit transfers. On an operational level, the addition of pseudo PANs poses no issues for the EFT networks because respective BINs for pseudo PANs are entered on EFT data bases allowing the pseudo PAN to be treated the same as any other PAN. NYCE mandates that PANs be input twice to eliminate entry errors. Both entries must match for the transaction to proceed.

FIs that don't adopt pseudo PANs need to take additional care in educating customers about appropriate authentication procedures, such as never to use a PIN, CVV2 (the three-digit number on the back of a debit card in the white signature area) or card expiration date in identifying a transaction.

¹³ See *BITS Framework for Managing Technology Risks for IT Services Provider Relationships* at www.bitsinfo.org.

¹⁴ According to STAR, FIs are generally very good at working together and arriving at equitable solutions to fraud issues.

- **Transaction Risk.** Transaction risk occurs when the transaction is denied for reasons such as NSF or when the transaction is not authorized by the user. Transaction risk can be addressed via:
 - Automated transaction monitoring and behavior-based logic systems;
 - Automated deferral of suspicious transactions;
 - Real-time pattern and velocity screening;
 - Automated methods to adjust for NSFs, administrative returns and notifications of change to limit processing exposure; and
 - Strict account- and user-level controls to guard against persistent and exponential fraud.
- **Technology and Infrastructure Risk.** These risks arise from system intruders, viruses and the like. They can be addressed by establishing secure systems with strong encryption or through SAS 70 and multiple security audits of the service provider or by participating FIs. Given the potential volumes and velocity of A2A transfers, robust security is critical. BITS members have noted the need to increase security to accommodate increased activity and related risks.
- **Regulatory and Compliance Risk.** These risks occur when the FI fails to comply with relevant rules and regulations. These risks can be addressed by adhering to relevant rules and regulations, including the Bank Security Act, the USA Patriot Act, OFAC, NACHA's operating rules, GLB, FCRA, and Regulation E.
- **Fraud Risk.** Though fraud perpetrated on an A2A transfer doesn't constitute new abuses, the velocity and volume of A2A transactions across FIs gives rise to potentially serious increases in fraud. FIs need to be aware of A2A volumes and should use operational systems to monitor increased transaction flows.

FIs should review their fraud policies to make sure that A2A transactions are being scrutinized at least to the same level of detail as check and wire transfers. A call for a higher level of due diligence for these transfers may be in order.

Policies should be in place to incorporate A2A activity into Suspicious Activity Reports (SARs) as needed. With respect to disintermediation risk, the Working Group discussed the potential for A2A services to draw demand away from higher margin wire products. Given the dollar limits on A2A—NYCE, for example, restricts transactions to transfers of less than \$10,000—on average A2A transfers fall below the market for wire services and are more likely to compete with services such as Western Union, Travelers Express/MoneyGram and other money transfer agents. Wires do, however, provide immediate availability and have an advantage over current A2A services not switched through real-time EFT networks. Most FIs align daily A2A limits with daily POS limits (generally not more than \$2,000), although an FI could develop dedicated A2A limits.

Additional proactive measures by the networks and processors related to real-time monitoring of A2A (just as in non-A2A transactions such as offline debit and ATM/POS cash withdrawals) include account-specific reviews of transaction velocity, amount, venue, time of day and average daily balance. Capabilities will need to be further developed as transaction growth increases.

Adjusting and maintaining controls over limits on A2A transfers provides another means of managing risk. For example:

- **Funds Transfer/Dollar Limits.** These limits must be established. Limiting the dollar amount of transfers reduces fraud-related risks, particularly when the funds are moving to accounts outside of the originating institution. NYCE and STAR have defined maximum transaction amount thresholds,

but FIs alone determine daily withdrawal limits.¹⁵ FIs have the right to establish A2A-defined limits at their discretion and should set limits from the institution down to the individual end-user level. The sending FI is responsible for ensuring that all initiated transfers are within all established dollar limits. **The receiving FI could develop a system trigger based on a credit transfer to flag any transfers that do not meet regulatory rules.** The receiving FI could then initiate a chargeback to return the funds to the sender.

FIs should note that, technically, the network dictates that incoming credits must occur, regardless of the incoming FI's daily limits on incoming funds. Network rules could be amended to reflect an FI's stipulated limit, but at this point the FI is bound to receive funds sent. The FI could establish a hold on amounts over a set daily incoming limit and include an FI disclosure to cardholders on this point. Such an approach would require the FI to add code to recognize over-the-limit transfers.

- **Network Monitoring.** During the first quarter of 2005, specific risk-monitoring tools will be applied by some real-time EFT networks to monitor A2A transactions in near real time. Specific monitoring attributes include velocity, dollar amount, source and location of initiation and destination, and other trigger attributes. At this time, each network is pursuing proprietary monitoring solutions to mitigate potential risk factors associated with both sending and receiving A2A transactions.

A2A transactions are generally used for lower dollar amounts than the average wire transfer and as a consequence requirements for A2A fraud deterrents have not been as strong. Differences between rules governing wire and A2A transfers should be considered. For instance, in a wire transfer, the FI needs to be able to furnish a valid address on request (not a P.O. Box) for the payee, while with an A2A transfer the sending bank has no knowledge of the recipient's address.

Regulations

Regulatory requirements around A2A will evolve and are expected to expand. Each institution should conduct internal due diligence to make sure it is in compliance with current money transfer regulations. **FIs should consider proactively invoking the Bank Secrecy Act's Travel Rule, which states that a bank must maintain a record of each funds transfer of \$3,000 or more that it originates, acts as an intermediary for, or receives.** The amount and type of information the FI must record and keep depends upon its role in the funds transfer process. Also, an FI that acts as an originator or intermediary for a funds transfer must pass certain information along to the next bank in the funds transfer chain.

Exception Processing

Exception processing constitutes another area FIs should address when launching an A2A program. Increased volumes may require automated returns processing, which may require an upgrade in FI operations.

Authentication

As in any FI-initiated payments transaction, the sending FI must authenticate the sender upon opening the account and on every A2A transaction. For account opening, some service providers use a process of sending a verifying receipt of micro-deposits (deposits of a few cents) that can be used to validate non-host accounts. For ongoing transactions, the sender is always authenticated via PIN/magnetic stripe, ID/password, or other means, depending upon the A2A initiation device (i.e., ATM, e-banking, phone banking, and teller). In some cases, depending on the network, the sender can authenticate him or herself

¹⁵ These limits are usually aligned with POS values.

and initiate the funds transfer from another FI's platform, such as the ATM of another FI on the network.

Authentication is channel and entry device dependent. As with general online banking, ID and password are required for Internet and VRU access, cards and PINs are used at ATMs, and the FI sets requirements at in-branch locations. Card numbers should be stored in an encrypted database, as required by regulations.¹⁶ PANs are generally not stored anywhere, although the sending FI may store them in an e-banking application behind a separate firewall not accessible to end-user or outside use and encrypted to meet industry standards. (For more on authentication, see page 19, Functionality from the Customer's Perspective.)

Additional protections can also be established. Card number use may be restricted, for example, so that after set up the receiver card number must be truncated. STAR planned to require sending FIs to authenticate the recipient via a commercially reasonable process before providing the recipient's card number to the sender. The recipient name and truncated card number (or a pseudo identifier) would then be placed on the approved transfer/biller list for the sender. FIs requested flexibility so they could select and implement the risk management process appropriate to their institution. The network amended its rule to state that regardless of how the recipient card number was obtained, the card number—if listed on the transfer/payee list—must be truncated to the last four digits.

Options for more secure network access to customer accounts include the Universal Payment Identification Code (UPIC). The UPIC concept was developed and implemented by The Clearing House in response to recognition that a credit-only, surrogate DDA account number might be useful in a rapidly evolving electronic banking environment.

UPICs are used and maintained by FIs. Currently, UPICs function only in the ACH environment, but the framework is compatible with PAN-based routing and could be used to create a pseudo (credit-only) PAN for use on real-time systems. UPICs provide additional security by eliminating the use of actual account numbers and allowing only credit payments to accounts by blocking debit payments. UPICs were developed to drive the acceptance of electronic payments and are used in conjunction with a universal routing number that allows for broad-scale application of UPIC-based transfers.

Future applications of the UPIC may create opportunities for FIs. Alternate uses for a UPIC-based routing table in the context of developing improved risk tools within the payments space could be developed. The UPIC could help forge cross-network connectivity with ATM networks and establish a broader reach for real-time A2A functionality.

Another option for more secure network access to customer accounts is the DDA-associated pseudo-PAN. The sending FI can also require that the recipient consumer only provide his or her PAN to an automated system individual voice recognition unit (IVRU) or an FI customer service representative, thereby preventing the sending consumer from viewing the account number. The sending FI would only list the recipient's name or other identifier to the sender. This is the method STAR initially envisioned; the network plans to issue a rule pending approval by its FI advisory board. STAR's member FIs prefer to manage these details independently.

¹⁶ The STAR network, for example, has an operating rule to this effect.

Mechanics

To effect an A2A transfer, the FI, in conjunction with third party providers, processors and/or networks must allow for account setup and access and transaction reporting or notification procedures.

- User account setup access:
 - Sender sets up receiver details through a device provided by his or her FI (website, VRU, ATM, teller).
 - Receiver's cardholder number can be entered directly by sender, or sender's FI can require receiver to provide the number in some other manner. (This is the sending FI's decision.)
 - Prior to allowing the sender to initiate a transfer transaction, the sending FI must perform identity verification of the sender and of the receiver as required by applicable law, including the BSA and OFAC.¹⁷
 - The sending FI activates transfer capability on behalf of the sender. STAR requires pre-registration; NYCE does not. For NYCE cardholders, once the FI is certified, the cardholder may transact at any FI or foreign ATM where sending capability is available.

- Transaction details provided:
 - ACH or PIN-less credit. (With the NYCE service, ACH is not an option.)
 - Submitted from Internet, VRU, branch or ATM.
 - Sending FI debits sender's account ("on-us").
 - Sending FI routes credit via specified network to the receiving FI.
 - Unique Regulation E information in online transaction, as provided by the sending FI. (Provision of the sender's name is optional. At a minimum, the PAN, transaction dollar amount, transaction date and transaction identifier are required.)
 - Utilize existing settlement and reporting infrastructure.

- As with all procedures executed in volume, uniform standards enhance efficiency, functionality and prospects for growth.

From the customer's perspective, A2A functionality varies based on the access point. Below are the steps to a Web-based transfer. After registering with the FI for A2A service (a one-time process), the customer:

- Logs on to the FI's (sending bank's) website.
- Completes an online authentication process (an access-point and channel-dependent process).
- Requests an intra- or inter-bank transfer (depending on the FI's capability and the consumer's need).

The sending FI then:

- Processes an "on-us" debit to the customer's account.
- Initiates a credit using the receiver account holder's PAN.
- Routes the credit through the network to the receiving FI and posts to the respective account.

On the STAR network, the transaction is approved or declined and funds are settled in real time (if EFT networks transport the transaction) or within one or two business days (if the ACH network is used for transport). For transactions that flow across the NYCE network, approval is granted once the FI attempts sending of pinless credit. If the attempt fails, the cardholder is informed immediately via a screen message indicating the receiving FI account is not available.

¹⁷ STAR considers this step to be registration. STAR does not have a rule regarding activation.

Some notable differences exist among services provided from alternate channels. For example, the authentication process in an ATM-based access generally requires the consumer to provide a two-factor authentication to initiate the transaction. In December 2004, the FDIC issued a strong recommendation that FIs call for two-factor authentication for online banking. However, no requirement currently is in place. Two-factor authentication in an ATM environment is governed by the payments network through which the transaction is routed. Likewise, e-banking requires an ID and password. No additional tokens are required by the networks. However, the FI may want to add additional tokens or challenges such as cardholder's date of birth or mother's maiden name. The same principles apply to telephone banking. The cardholder requires ID and password to engage.

Real-Time EFT A2A Transactions vs. ACH-Based Transfer Services

Transfers conducted over an ATM network offer several advantages:

- Two-factor (or two-token) authentication at some access points
- Real-time availability (net settlement occurs the morning of the following business day)
- Finality (no return or rescission)
- Significant revenue and service opportunity (a superior alternative to wires for low-dollar transactions)

These transfers also have limitations:

- Currently, they lack ubiquity. Today the ACH has significantly broader reach than real-time solutions.
- Transaction size is limited. Dollar limitations for outgoing funds are generally tied to daily POS withdrawal limits. There are no network rules or technical limitations requiring an FI to establish separate A2A dollar limits. Individual FIs can establish their own rules; today most FIs are commingling the A2A daily outbound limit with POS daily outbound limit.

III. THE FUTURE OF A2A FUNCTIONALITY

A. Nascent Technology: Opportunities for Growth

The A2A market has grown considerably since the BITS A2A Working Group was established. Increased demand is driven by consumer familiarity with electronic payments, including online auction services such as PayPal, which has experienced exponential growth since its inception in 1998. Bundling A2A functionality in combination with aggregation services (now routinely bundled into home banking platforms) is another avenue of expansion. Also, younger consumers are more inclined to select electronic or online payment, making A2A a growth opportunity from a purely demographic standpoint.

B. Levers

A number of tools are available to FIs that will help shape the future of A2A transactions. Among the most important in the short term are:

- Influencing EFT network interoperability to improve reach;
- Encouraging A2A activity on the part of the major card associations to enable enhanced national and international connectivity; and
- Promoting cross-channel adoption of discrete, credit only, DDA account identification techniques.

Interoperability

FIs that offer A2A services can leverage these overall market factors by using their influence to promote feature functionality that will further enhance adoption. The BITS A2A Working Group has identified real-time network interoperability as a key factor in developing a more robust A2A market. As the market develops, networks should be encouraged to adopt policies that allow inter-network switching via network gateways. That capability will expand considerably the reach of an FI's real-time A2A service and is viewed by the Working Group as mandatory for broad-scale adoption of A2A.

Role of Card Associations

The role of the major card associations in A2A services may offer opportunities to FIs. MasterCard and Visa both support A2A functionality in the EU. The functionality of Visa's Visa Direct product will enable transfers to accounts using the Eurogiro network in 2005. MasterCard's MoneySend product claims to accomplish transfers faster than any other service.

Both associations are building considerable A2A experience, albeit outside of the U.S. Two points are important here:

- National associations can quickly pick up the slack if NYCE, STAR and other regional EFT networks don't develop gateway service to provide substantially improved reach.
- Either association can, within legal limits, enable international real-time A2A transaction service when it believes the market is ready.

Discrete, Credit-Only DDA Account Identifiers

Adoption of credit-only DDA account number surrogates addresses a major consumer security concern, has the potential to reduce fraud, and—if implemented on a cross-channel basis—could significantly speed the adoption of A2A functionality. The Working Group believes that the UPIC approach to this issue is an attractive cross-channel candidate assuming that reasonable terms and conditions can be negotiated with the program's developer. Other applications of UPIC may also create opportunities for FIs. For example, a UPIC-based routing table may enable easier development of improved A2A risk tools.

C. Challenges

Among the challenges to be addressed in promoting FI A2A services is the perception that these products cannibalize higher margin services and increase prospects for money laundering and other fraud related schemes, particularly in the online environment.

Cannibalization

Cannibalization of higher margin products was raised by a few Working Group members as a concern in promoting A2A. Early A2A experience at the real-time EFT networks suggests that this concern is overblown. Average transfer amounts have remained below \$500. Although some small-value wire transfers may be disintermediated by a robust A2A functionality, this effect should be negligible because the majority of wire transfers are for amounts in excess of A2A network limits.

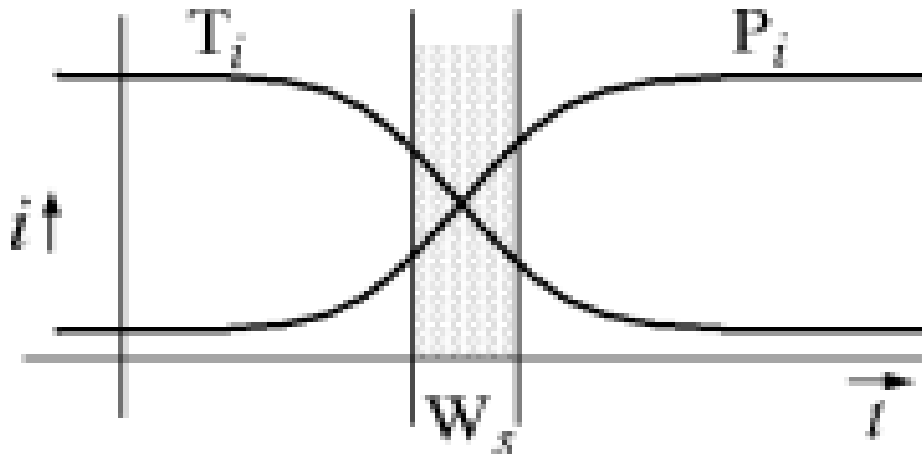
Fraud Detection

The growth of A2A connectivity will create challenges for FIs and networks alike. As the service grows, fraud attempts are expected to increase given the both the volume and speed of A2A transfers. FIs are appropriately concerned with the potential for increased money laundering and should exercise higher

levels of vigilance and consider implementing more robust fraud filters as A2A activity increases within their institutions. Recommended methodologies are outlined above: tracking by channel, initiation point and product, and developing a matrix to highlight the source of irregular activity.

APPENDIX

OPTIMUM TIME FOR STANDARDIZATION



Source: Mellon Financial Corporation

- The i axis describes level of interest and the t axis describes time. T_i describes technical interest, and P_i describes political interest.
- As time passes, technical activity declines as the technology becomes understood. Similarly, generally fueled by economic pressures, the political interest in a technology increases in some period. For a standard to be usefully formed, the technology needs to be understood: technological interest needs to be waning. But if political interest in a standard becomes too large, the various parties have too much at stake in their own vested interest to be flexible enough to accommodate the unified view that a standard requires.
- In this model, W_s is the “window of standardization” where technical interest is waning (i.e., the technology has become understood), but the political situation hasn’t become too hotly contested for constructive negotiating.