

THE PARTNER GROUP THIRD PARTY PAYMENTS SYSTEM ACCESS CONTROL

WHITE PAPER AND RECOMMENDATIONS

The Partner Group's Third Party Payments System Access Control Working Group was formed to develop common payments system access processes and standards relating to third parties (merchants, independent sales organizations, third party entrants, etc.). The Working Group has initially focused on processing and sales entities, including Independent Sales Organizations (ISOs), and third party entrants. The Group has identified key areas where it believes selective rules harmonization relating to third party payments system access will result in fraud reduction, safeguarding the safety and soundness of healthy competition in the payments industry.

April 2007

THE PARTNER GROUP

THIRD PARTY PAYMENTS SYSTEM ACCESS CONTROL WORKING GROUP WHITE PAPER AND RECOMMENDATIONS

APRIL 2007

ABOUT THE PARTNER GROUP

The Partner Group is a financial services industry working group formed in the fall of 2005 to address emerging payments risk issues that cross retail payment applications. Its members include BITS, Early Warning Services LLC, FSTC, ICBA, MasterCard, NACHA, NYCE, The Clearing House, STAR, VISA, and Federal Reserve Bank Payments Staff. Additionally, there are three bank members: SunTrust, Wells Fargo, and Wachovia. In the summer of 2006, The Partner Group chartered three working groups and invited additional financial institution participation on those work teams:

- Improved Fraud Information Sharing Working Group
- Liability Flows Among Networks Working Group
- Third Party Payments System Access Control Working Group

About the Improved Fraud Information Sharing Working Group

The Improved Fraud Information Sharing Working Group was formed to identify and encourage the sharing of key data that might best reduce the forms of fraud that migrate from one payment application to another. The Working Group's purpose is to develop improved fraud reduction information-sharing capabilities among payments Networks in different silos. This work team is co-chaired by Glen Sgambati, Chief Data Officer, Early Warning Services LLC; and Ward Gailey, SVP, SunTrust.

About the Liability Flows Among Networks Working Group

The Liability Flows Among Network's Working Group's goal is to document current liability gaps among Networks and develop workable approaches to close those gaps. This Working Group is developing and evaluating approaches to better manage inter-Network liability when a specific rules violation has extended consequences outside of the Network where the violation occurred. The Liability Flows Among Networks Working Group is co-chaired by Beth Lynn, Senior Vice President, STAR Systems; and Timothy Boike, Vice President, Wells Fargo.

About the Third Party Payments System Access Control Working Group

The Third Party Payments System Access Control Working Group was formed to develop common payments system access control processes and standards, as appropriate, relating to third parties (merchants, independent sales organizations, third party entrants, etc.). The Group's initial goal is to document and define approaches to close the most addressable access control gaps. The team is co-chaired by Cary Whaley, Associate Director, Payments and Technology Policy, ICBA; and Lou Anne Alexander, SVP, Wachovia. In addition to the co-chairs, the Third Party Payment System Access Control Working Group's membership includes:

- Al Briand, The Bank of New York
- Jackie Buchannan, T&C FCU
- Peter Burns, FRB Philadelphia
- Keith Crockett, Compass
- Don Devine, STAR
- Joseph Flannery, BB&T
- Jeanette Fox, NACHA
- Mike Gorski, VISA
- Lynne Karla, Huntington
- Ian Macoy, NACHA
- Jim McKee, FRB Atlanta
- Tim Mills, EPN
- Leslie Mitchell, NACHA
- Susan Pandy, NACHA
- Hector Rodriguez, VISA
- Frank Sardina, EPN
- Victoria Strayer, TSYS
- Bruce Sussman, NYCE
- Larry Taft, Midwest Independent Bank
- Sam Vallandingham, First State Bank

This project was managed by The Santa Fe Group on behalf of BITS. Funding was provided by a group of BITS member financial institutions. Paul Tomasofsky of Two Sparrows Consulting Group provided invaluable assistance to the work group in a number of areas. Tom Hemnes and Rick Brunell of GTC Law Group LLP served as counsel. Matt Ribe and Gary Roboff of BITS served as consultants to The Santa Fe Group on this project, and, with Cheryl Charles of BITS, facilitated the Working Group's efforts.

In the course of its work, the Third Party Payments System Access Control Working Group formed sub teams to explore four areas in depth:

- The **Registration** Team was chaired by Don Devine of the STAR Network.
- The **Underwriting** Team was chaired by Joe Flannery of BB&T.
- The **High Risk** Team was chaired by Sam Vallandingham of First State Bank, Barboursville, WV.
- The **Information Security** Team was chaired by Victoria Strayer of TSYS.

BACKGROUND

Several incidents in the last few years have highlighted the need for greater industry due diligence in enabling and maintaining payments system access for third parties of all types. Not surprisingly, as financial institutions (FIs) have increasingly relied upon third party Agents to sell and provide payments system access, it has become a greater challenge to ensure consistent due diligence about the specific parties on whose behalf FIs enable payments system access. Examination of rules structures in a variety of payments networks (“Networks,” as defined below) has shown that there is significant variation in how Networks govern third party payments system access. Additionally, there are inconsistencies in the amount of information available to Network administrators concerning third party activities within the Networks in which they operate. In some situations, this lack of information has led to increased losses across multiple payments systems. The Third Party Payments System Access Control Working Group has identified key areas where it believes selective rules harmonization relating to third party payments system access will result in fraud reduction. Throughout its work, the Group has sought to ensure that its recommendations will preserve or enhance the ability of financial institutions of all sizes and other payment network participants to compete in an environment where adherence to best practice standards is becoming more and more important.

The third party access recommendations in this paper are designed to apply in “open” payments Networks where financial institutions routinely have a contractual responsibility on each side of a transaction, as Issuers and Acquirers or as Receivers and Originators. The vast majority of electronic payments in this country are made through Networks where FIs play those roles, but that liability structure is not universal. In some Networks, such as American Express or Discover, the Network itself assumes the contractual responsibility that FIs have elsewhere.

Recommendations are intended to be taken at a strategic level, and are crafted by design to give networks flexibility in honing specific direction (for example, around the frequency of continuing underwriting due diligence) based upon specific circumstances in each risk environment.

For ACH transactions, the recommendations are directed towards third parties who primarily process ACH debits. Some of these recommendations may not be appropriate for traditional credit-only third parties, such as payroll processors or bill payment service providers. Credit origination risk is very short term, highly quantifiable and much more manageable than debit origination risk. That said, there may be risk in certain credit origination situations. For example, small or start-up payroll and bill payment service providers certainly present the type of risk these recommendations are designed to minimize.

The Payments Risk Competency Framework may have broad application potential across the industry, especially in remedial situations. Further, the matrix may be a powerful educational tool for any financial institution engaged in the payments business, useful for both self assessment purposes and for assessing business partners.

Glossary of Terms

To bridge silo-specific vocabularies, the Working Group found it necessary to create several specially-defined terms that may be unfamiliar to industry participants. For example, the term “Sponsor” is used to identify both Originating Depository Financial Institutions (ODFIs in the ACH) and Acquiring Financial Institutions (commonly referred to as “Acquirers” in card Networks).

As used in this paper, the following terms have the meanings indicated.

ACH Operators (also referred to as **Operators**) play the role of Network “switch” in the ACH. ACH Operators receive transactions from Originators and deliver the transactions to receiving institutions at scheduled intervals. There are currently two Operators, Federal Reserve Payments Services and EPN (The Clearing House).

Acquirers provide credit and debit card processing, billing, reporting, settlement and operational services to their customers, usually merchants or other entities providing a good or service..

Agents are entities which Sponsors or Processors may engage to perform due diligence (for example, on-site inspections) on their behalf. When a Sponsor or Processor contacts with an Agent to perform these functions, it retains its responsibilities under network rules to perform due diligence and to use information it obtained through that process appropriately. Non-financial institution sales agents, for the purposes of this paper and as noted below, are Processors, not Agents.

AML stands for Anti Money Laundering regulations and practices.

Direct Connect Processors are authorized by their Sponsors to send transactions on behalf of others directly to ACH Operators or to Real Time EFT Networks. Transactions sent to ACH Operators by Direct Connect Processors contain a record of the Sponsor’s Routing-Transit (RT) number. In the ACH, Processors may obtain an Electronic Transaction Identifier (ETI), which enables identification of transactions sent under the Processors’ auspices. Individual merchants may obtain direct access, but they do not fall within the definition of Direct Connect Processors for purposes of these recommendations as long as they are not sending transactions on behalf of other entities.

Electronic Transaction Identifiers (ETIs) are special purpose routing numbers designated for use as electronic addresses of organizations which are not banks but process payments transactions on behalf of banks. (*ABA Definition*)

Gateway Agreements between real-time EFT networks may provide access to one network’s endpoints to members in another through a single access point established by mutual agreement between the two networks. Gateway Agreement terms and conditions vary widely.

High Risk identifies relationships or entities that represent increased reputation, credit, strategic, liquidity and transaction risk. High Risk entities include companies with one or more of the following characteristics:

- Historical association with criminal elements
- Difficult authentication characteristics, particularly in Internet commerce
- Historically high rates of return or disputes
- Poor credit or difficult to verify creditworthiness
- Reputation or compliance risk associated with the business

Please see section 3.1 for further detail and for illustrations.

Issuers are financial institutions that provide credit or debit cards and associated accounts to their customers.

Network, unless otherwise indicated, means both real time and batch payments processing systems in which financial institutions routinely have a contractual responsibility on each side of a transaction, as Issuers and Acquirers or as Receivers and Originators. In the ACH Network, rules are developed and maintained by the National Automated Clearing House Association (NACHA). Two Operators, Federal Reserve Payments Services and EPN (The Clearing House) clear and settle transactions. In Real Time EFT Networks, governance and operating components (including the Network switch) are typically integrated into a single entity.

Next Tier Processors are Third Parties that process payments but are not Direct Connect Processors. These parties are often referred to as merchant aggregators, ISOs, or third party senders. Processing entities that participate in Real Time networks exclusively through Gateway Agreements are not Next Tier Processors.

Originating Depository Financial Institutions (ODFIs) are the institutions that receive payment instructions from Originators and forward the entries to an ACH Operator. *(NACHA definition)*

Originators are the entities that agree to initiate ACH entries into the payment system according to an arrangement with a Receiver. The Originator is usually a company directing a transfer of funds to or from a consumer's or another company's account. *(NACHA definition)*

Processors are FI's and Third Parties that process payments routed through networks. They include both Direct Connect Processors and Next Tier Processors. Merchants are not Processors.

Receivers are natural persons or organizations which have authorized an Originator to initiate an ACH entry to the Receiver's account with the RDFI. A Receiver may be either a company or a consumer, depending on the type of transaction. *(NACHA definition)*

Receiving Depository Financial Institutions (RDFIs) receive ACH entries from the ACH Operator and post the entries to the accounts of its depositors (Receivers). *(NACHA definition)*

Real Time EFT Networks are financial Networks that route transaction requests to and from an authorization host in real time. These are typically card-based Networks, such as VISA, MasterCard, STAR, PULSE, and NYCE.

Registration means (i) identification of Processors in a contract between a Sponsor and an ACH Operator or a Real Time EFT Network or (ii) a separate form filed with an ACH Operator or with a Real Time EFT Network identifying Processors and providing such other information as required by the Operator or Real Time EFT Network.

Sponsors are generally financial institutions that assume liability for entities on whose behalf they enable payments system access. These are Originating Depository Financial Institutions (ODFIs) in the ACH, and are generally (with a few exceptions) Acquiring Banks in real time EFT Networks. Some Networks allow other Networks to act as Sponsors of other entities in limited circumstances (such as through Gateway Agreements).

Third Parties refers to non-financial institution processing entities or sales agents. They include aggregators, direct or Next Tier Payments processors, ISOs, Third Party entrants or senders, etc.

RECOMMENDATIONS

The Partner Group recommends that Networks incorporate rules consistent with the following principles, adapted to each Network's unique business model, organizational structure, and policies. It is expected that the actual implementation of these recommendations will vary from Network to Network. Potential members of Networks will continue to make independent judgments about which Networks provide the best vehicles for their payments businesses.

The recommendations that follow are designed to apply in "open" payments Networks where financial institutions routinely have contractual obligations on each side of a transaction, as Issuers and Acquirers or as Receivers and Originators. The following recommendations relate to managing Network risk created by Third Party Processors (or ISOs) that are sponsored into payments Networks. The Third Party Access Working Group recognizes that AML issues have not been addressed in these first stage recommendations; AML recommendations will follow in the next phase of work.

1.0 Registration Recommendations

Although one of the most basic safety and soundness principles is that Real Time EFT Networks should know each of the entities operating in their systems, today that is not universally the case. When fraud arises, preventable harm may be caused if Sponsors and Networks cannot readily identify the transaction source. The Third Party Payments System Access Control Working Group recommendations that follow aim to close registration-related gaps while respecting the structural differences between card-based EFT systems and the ACH.

1.1 Registration: All Networks – Each Network should ensure that all transaction messages contain information identifying the Sponsors.

Rationale: This recommendation enables Sponsors to identify the transactions for which they have responsibility, which in turn permits them to monitor for excessive returns or other noteworthy changes in transaction mix within an appropriate time frame. This recommendation recognizes the importance of ascertaining the sponsoring relationship associated with each transaction on a timely basis.

1.2 ACH Registration - Contracts between each Sponsor and each Operator must identify all Third Party Processors that are using the Sponsor's routing-transit number to connect directly to the operator. In addition, the ACH Network should review and consider establishing additional registration requirements for Next Tier Processors (e.g., aggregators, indirect or other payment processors) behind Direct Connect Processors. At a minimum, all sending and receiving points behind Sponsors, Direct Connect Processors, and Next Tier Processors should be known to the Sponsor and such information should be readily available to the ACH operators and NACHA upon request.

Rationale: From a safety and soundness perspective, it is important that each Operator maintain a record, through the Sponsor, of each processing entity on whose behalf the sponsor is enabling payments system access. Most often issues arise with Next Tier Processors..

1.3 Reliable ACH Payee Identifier: The ACH network should take appropriate steps to ensure that Sponsors and Processors cause any company name appearing in an ACH record

to be a name readily and reliably identifiable by the Receiver as the payee of the transaction. A method to contact each payee should be included in the ACH record where appropriate.

Rationale: In today's ACH environment the payee of record can often not be uniquely and reliably identified from information contained in the transaction record. The inability to identify a payee increases risk significantly

1.4 Registration: Real Time EFT Networks - All Processors and firms that are aggregating entities (such as ISOs) behind Processors must be known to the Network on an ongoing basis. Networks may implement different processes to achieve that goal. For example, some Networks will require contracts with any and all processing entities (except those behind Gateway Agreements), while others will simply register Third Parties. Any approach that achieves the goal is satisfactory.

Rationale: Basic safety and soundness considerations make it important for every Network to identify and evaluate each Third Party (and any Processor that is a customer of the Third Party) on whose behalf it is enabling payments system access. Issues are commonly related to Next Tier Processors.

2.0 Underwriting Recommendations

Ensuring proper initial and ongoing underwriting due diligence is essential to ensuring a safe payments environment. As retail payments functionality has converged, bad actors have begun to troll the payments system, seeking the point of least resistance for payments system access. While every Network has high level underwriting requirements (and some have extremely detailed guidance about how reviews must be accomplished), harmonization of key underwriting elements could reduce the risks from payments "trolling," benefiting all stakeholders. This section incorporates references to High Risk recommendations where appropriate.

2.01 Sponsorship Requirements: Capital - Each Network should develop its own capital standards for Sponsors that bring Third Parties to the Network. Rules should ensure that capital reviews look across Networks to determine whether capital is being exposed in multiple Networks. Sponsors that do not meet the capital standards may nevertheless qualify, at the Network's discretion, by purchasing insurance or establishing risk-mitigation related competency. (See 2.02 *Payments Risk Competency Framework*.)

Rationale: These recommendations acknowledge that smaller financial institutions must have cost effective means to qualify to sponsor specific transactions in situations where their base capital positions might not be adequate to enable them to sponsor appropriate business entities. There are a number of ways through which a Sponsor might meet sponsorship requirements.

2.02 Sponsorship Requirements: Payments Risk Competency Framework - The goals of the Payments Risk Competency Framework are, at a Network's discretion: (1) to provide a means for Sponsors that do not meet capital requirements to qualify for participation in payments systems by establishing their competency to mitigate risk; (2) to provide competency requirements that may be used as an alternative to capital requirements in High-

Risk environments; (3) to provide a remedial approach to permit Sponsors that have been responsible for losses to re-establish their competency; and (4) to enable financial institutions of all sizes to compete as Sponsors, provided they establish and verify competency to manage payments-related risks.

Levels 4 and 5 competence must be established by an independent audit or review. The Network, in light of the risk profile of the payments and other relevant factors, should determine the scope and nature of the independent audit or review.

The Payments Risk Competency Framework seeks to measure competence in these areas:

- *Skills and Expertise* - The commitment to developing a common body of knowledge through training and knowledge-sharing.
- *Awareness and Communication* - The ability to recognize payments issues and effectively communicate them to their organization.
- *Policies, Standards, and Procedures* - The ability to document, codify and follow sound operating procedures.
- *Risk Measurement & Analysis* - The metrics employed to identify and measure risk.
- *Audit and Competency Level Assessment* – The independent verification of an organization’s level of risk management effectiveness.
- *Tools and Automation* - The tools needed to identify and monitor risk.

2.02a High Risk Payments (see 3.1) - At the discretion of a Network, Sponsors that originate and process High Risk payments must have a minimum of level 4 competency for each category.

2.02b Over Capital - At the discretion of a Network, Sponsors that wish to originate and process payments in excess of that permitted by their capital, under relevant Network rules, may nevertheless qualify by having at least a level 4 competency in each category.

2.02c High Risk Payments over Capital Adequacy - At the discretion of a Network, Sponsors that originate and process High Risk payments above their capital may do so if they demonstrate level 5 competence in each category.

2.02d Remedial Use of Risk Competency Framework - Networks can recommend performance tier requirements to Sponsors as a remedial measure if the Sponsor has a history of significant rule violations.

Payments Risk Competency Framework						
Payments Risk Competency Level	Skills and Expertise	Awareness and Communication	Policies, Standards and Procedures	Risk Measurement and Analysis	Audit and Competency Level Assessment	Tools and Automation
	Skills required for effective payments mitigation are not identified. A training plan does not exist and no formal training occurs.	Recognition of the need for the payments risk mitigation process is emerging. There is sporadic communication of the issues.	There are ad hoc approaches to payments risk mitigation processes and practices. The processes and policies are not consistently defined.	No processes exist to measure the source, magnitude and direction of payments risk, either from new or legacy products or services. Management is unaware of the cost of compliance vs. the cost of inaction vs. the risk.	Independent assurance over key business and technical processes is not performed. Competency level assessment. Self assessment.	Some payments risk mitigation tools may exist. Usage is based on standard desktop. There is no planned approach to the tool usage.
Level 1	Minimum skill requirements for effective payments mitigation are identified for critical areas. Training is provided in response to needs or events, rather than on the basis of an agreed plan, and informal training on the job occurs.	There is awareness of the need to act. Management has begun to communicate regularly on payment system risk mitigation issues.	A consistent set of risk mitigation processes begins to emerge, but are largely intuitive. Some aspects of the process are repeatable because of individual expertise and some documentation. Informal understanding of policies and procedures may exist.	Management begins to reactively assess payments risk inherent to existing operations, products and services. A knowledge base of payments risk accrues to those who produce the initial assessments but it is not well understood outside of the local project team.	Management and the Board are aware that external stakeholders (key customers, regulators, investors) require independent assurance. However, there is little perceived value in independent audit until it becomes mandatory. Competency level assessment. Internal, more formal.	Common approaches to the use of payments risk mitigation tools exist but are based on solutions developed by key individuals. Vendor tools may have been acquired, but are probably not applied correctly, and may even have not been used.
Level 2	Skills requirements, including the development of a payments risk mitigation common body of knowledge, are defined and documented for all areas. A formal training plan has been developed, but formal training is based on individual initiative.	There is understanding of the need to act. Management effectively communicates the overall issues, including those arising from changes to payment network rules, new or revised regulatory guidance, technology trends, etc.	Use of good practices has emerged. Payments risk mitigation processes, policies and procedures are appropriately defined and documented for all key activities. Formal understanding of policies and procedures exists.	Management begins to proactively develop payments risk tolerances, limits, policies, procedures and objectives. Formal responsibility for measuring and reporting risk is assigned. Ad hoc tools are used to acquire data used for risk management.	Management becomes acclimated to the requirements (frequency, issues, documentation request) of independent auditors. Management begins to allocate internal resources to hire internal auditors, payments risk management specialists, and to codify key policies. The organization begins to think "what will the auditors" say. Competency level assessment. Independent audit.	A plan has been defined for use and tools have been standardized to automate the payments risk mitigation process. Tools are being used for forensic purposes, but may not all be in accordance with the agreed plan, and may not be integrated with one another.
Level 3	Skills requirements are routinely updated for all areas, proficiency is ensured for all critical areas and certification is encouraged. Mature training techniques are applied according to the training plan and knowledge sharing is encouraged. All internal payments risk mitigation experts are involved and the effectiveness of the training plan is assessed.	There is understanding of the full set of payments risk mitigation requirements and the need to keep staff current about material changes that could impact the payments business. Mature communication techniques are applied and standard communication tools are in use.	Payments risk mitigation process is sound and complete. Internal best practices are applied across multiple areas of the business. All aspects of the process are documented and repeatable. Policies have been approved and signed off by management, including the board of directors. Standards for developing and maintaining the processes and procedures are adopted and followed. Periodic review is required.	Formal metrics are reliable, disseminated, and used to manage tolerable payments risk. Data analysis tools evolve from ad hoc to either off the shelf or robust in-house solutions. Processes for capturing new types of payments risk are reliable and extended before entry into new businesses or association with new partners.	Internal audit and risk management are viewed as partners with management in sensible risk taking and in payments risk avoidance. Management policies and board committee documents clearly indicate that management is ultimately responsible for limiting risk and for controlling operative risk management policies and that effective practices are in place. Competency level assessment. External audit.	Tools are implemented in accordance with a standardized plan and some have been integrated with other related tools. Tools are being used in main areas to automate management of the process and monitor critical activities and controls. A wide range of payments risk mitigation techniques are used, with appropriate actions taken by management on a timely basis.
Level 4	The organization formally encourages continuous improvement of skills, based on clearly defined personal and organizational goals. Training and education support external best practices and use of leading edge payments risk mitigation concepts and techniques. Knowledge sharing is an enterprise culture and knowledge-based risk mitigation systems are being deployed. External experts and industry leaders are used for guidance.	There is forward-looking understanding of payments risk mitigation requirements. Proactive communication of issues based on trends exists, mature communication techniques are applied and integrated communication tools are in use. .	External best practices and standards are applied. Process documentation is evolved to automated workflow. Processes, policies and procedures are standardized and integrated to enable end-to-end management and improvement.	Payments risk management metrics increase in number and sophistication and may include online or real time tools. Enterprise wide monitoring and issue remediation is in place. A portfolio approach is used to identify and aggregate enterprise-level cross channel payments risks.	Internal audit and payments risk management practices are enterprise wide, repeatable and not dependent on key personnel or favorable business conditions. Audit tools and procedures reliably evolve and forecast over the horizon risks. Continuous monitoring is routine. Competency level assessment. External certified risk based audit.	Sophisticated payments risk mitigation toolsets are fully integrated across the enterprise to enable end-to-end support of the processes. Tools are being used to support process improvement and automatically detect control exceptions. The FI has the ability to monitor transactions seamlessly across channels. The entity is completely up to date with both regulatory requirements and any relevant regulatory guidance.
Level 5						

2.2.03 Background Check on Business and Principals - Sponsors are responsible for performing background checks on any Third Party handling customer payments data with whom they have a contract. Third Parties must cooperate with the Sponsor in completing those checks.

Initial Requirement: Sponsors must perform a background check on each Third Party with which they have a contract and in appropriate cases (for example, when a company is not publicly held) must perform a background check on the principals of that Third Party. Each Third Party must conduct a background check on each company for which it processes payments. **Ongoing Requirements:** Sponsors must conduct ongoing due diligence at regular intervals on the third parties for whom they enable payment system access.

Examples of key background check components follow.

Rationale: Background checks are essential components of good due diligence. Sponsors and their Agents should treat due diligence associated with enabling payments system access as they would any review before extending credit.

2.04 Financial Analysis – Initial Requirement: Financial analysis relevant to the processing requirements of the Third Party must be performed before Network access is enabled. Appropriately reviewed or audited financials should be part of such an analysis. Sponsors may implement a tiered level of analysis dependent on the volume and value of payments and the nature of the payments/returns being processed. It is a best practice to verify applicable business insurance policies to gain assurance that the entity will be viable in the event of a business interruption. **Ongoing Requirement:** Financial analyses must be performed at regular intervals. Sponsors should be notified of any changes to the type and scope of business insurance. **High Risk Requirement:** More frequent financial analyses of High Risk entities are appropriate and must be undertaken at shortened intervals appropriate to the specific situation.

Rationale: These recommendations seek a balance between explicitly requiring a financial analysis and prescribing, in detail, how that financial review should be conducted. The level of analysis should be predicated on the level of risk the Third Party's activities pose to the Sponsor.

2.05 Onsite Inspections – Initial Requirement: The Sponsor or its Agent must perform an onsite inspection before it enables network access. Inspections should have focused objectives consistent with the risks of the business. **Ongoing Requirement:** The Sponsor or its Agent must perform regular onsite inspections of Third Parties with which they have a contractual relationship. The Sponsor or its Agent must also perform regular onsite inspections of each merchant or other company for which it processes payments. Inspections should have focused objectives consistent with the risks of the business. **High Risk Requirement:** In situations where High Risk entities are involved, additional site visitation is often necessary. Further, additional skill sets may be required by those charged with making on-site evaluations. Sponsors should have a process in place to verify that onsite inspections are performed with frequencies and procedures appropriate to High Risk situations.

Rationale: Onsite inspections are another essential component of good due diligence. This recommendation recognizes that Sponsors may use Agents to conduct onsite inspections as part of initial and ongoing due diligence. In High Risk situations extra due diligence is required so that Sponsors better understand with whom they are dealing and how activities change over time. Onsite visits can be an effective preemptive step at removing bad actors before they enter a Network.

2.06 Verification of Onsite Inspections – Initial and Ongoing Requirement: Sponsors must be able to provide proof that inspections were properly conducted. Problems uncovered during on-site inspections must be resolved prior to the commencement or continuation of business. On-site inspectors must be appropriately qualified.

Rationale: The ultimate responsibility for ensuring that proper onsite inspections have been performed falls on the Sponsor, which assumes liability for the actions of its customers. Requiring the Sponsors to provide proof, on request, that inspections have occurred will help to ensure that Sponsors discharge this responsibility. This recommendation recognizes that Sponsors may use Agents to conduct onsite inspections, while addressing problems that have been caused by unqualified Agents.

2.07 Merchants: Verifying Nature of Business Operation – Initial Requirement: The Sponsor must verify that any merchant for whom it is enabling payments system access is actually in the business in which it claims to be. **Ongoing Requirement:** These reviews should generally be performed on an annual basis, but may be performed more or less frequently on a risk-adjusted basis (see High Risk recommendations; section 3.) Review frequencies should depend on the nature of the merchant’s business and the channel through which business is conducted. **High Risk Requirement:** High Risk businesses should be reviewed more frequently. Appropriate thresholds (such as unexpected changes in transaction volume or mix, return rates, etc.) might also trigger more frequent reviews.

Rationale: This recommendation is designed to minimize the likelihood that merchants will operate legitimate business “fronts” to conceal inappropriate activities.

2.08 Liability Associated with Sponsored Transactions – Ongoing Requirement: The Sponsor, not the Network, shall be liable for transactions the Sponsor introduces into the Network. Each Sponsor must implement procedures to monitor the Third Parties it sponsors. Those procedures should adequately reflect this responsibility, and should be consistent with any requirements established by each of the Networks in which the Sponsor participates.

Rationale: Payments Networks are not equipped to provide adequate due diligence for all entities that operate in their system. Extending access to the payments system is, in effect, an extension of credit to an entity, a role central to banking.

2.09 Downstream Activity Monitoring – Ongoing Requirement: Sponsors and Third Parties must monitor transactions for indications of risk issues within an appropriate time frame. Issuers and receiving institutions must also monitor transaction volumes and other risk indicators to mitigate loss when fraud occurs. Specific risk indicators and thresholds will vary on a situational basis, and on the basis of anticipated risks. Examples might include

changes to transaction volume, returned items and transaction mix. The industry should enable Sponsors in all Networks to monitor transaction activity in order to identify changes in transaction behavior.

Rationale: The Sponsor assumes the responsibility for all transactions submitted to settlement under its auspices, even if the entity generating the activity is several times removed from the Sponsor. Unusual patterns involving balance inquiries, denials, etc., may be harbingers of fraud.

2.10 Review of Other Network Relationships – Initial Requirement: Third parties must disclose all other Network relationships to their Sponsors, including relationships with other sponsors in the same Network. **Ongoing Requirement:** Each Sponsor should regularly review those relationships to verify the Third Party’s capital adequacy and that the Third Party’s experience level is appropriate to the risk it is taking. Each evaluation should take into account the number and scope of Network relationships. Third Parties must disclose to the Sponsor any compliance-related fine or penalty historically within a period of time established by the Network, and on an ongoing basis.

Rationale: Sponsors must understand the nature of every Third Party Network relationship, and how those relationships change over time. Third Party capital leverage is not static. As the number of spontaneous ACH debit transactions has increased, Third Parties increasingly operate in both ACH and Real Time EFT Networks. Third Parties may have relationships with multiple Sponsors, even within the same Network. Without regular review, Sponsors may not know changes in capital leverage. Information about an entity’s behavior in one Network may be relevant to the risks involved in sponsorship to another.

2.11 Record Retention and Maintenance – Ongoing Requirement: Sponsors and Processors must retain records related to the processing of transactions. These records must be retained for a period sufficient to achieve forensic and dispute resolution objectives, and as otherwise required by law or the Network.

Rationale: This requirement enables an effective audit trail. Without the assurance of reasonable transaction data storage, there can be no confidence in “after the fact” incident reconstruction. Record retention is a highly regulated area, and the recommendation is not intended to alter existing legal and regulatory requirements (Sarbanes-Oxley, Federal Rules of Evidence, etc).

2.12 Compliance with Network Rules, Regulatory Restrictions, and Applicable Federal, State and local Laws – Ongoing Requirement: Network Rules must stipulate that all Sponsors, Third Parties and Agents must comply with Network rules and with all applicable federal, state, and local laws and regulations. Networks should have processes in place to verify that participants comply with Network rules. **High Risk Requirement:** Sponsors must be prepared to take additional steps to monitor the regulatory compliance of entities for whom they provide network access. In some situations, monitoring of individual transactions may be required.

Rationale: This recommendation is designed to ensure that there is a contractual requirement for rules adherence for all Network parties, including those behind “principal”

members. In High Risk environments it may be necessary to determine whether items being purchased may be legally acquired on a transaction by transaction basis. There may also be different reporting and/or registration requirements. Online pharmacies and internet gambling are two examples of these High Risk environments.

2.13 Employee Policies – Initial and Ongoing Requirement: Each Third Party must implement, enforce, and make available to its Sponsor hiring and data handling policies appropriate to the nature of its business. At a minimum, background checks should be performed on any employee with access to payments related data. Best practice applications such as internal network segmentation and need to know access limitations should be used to complement hiring safeguards.

Rationale: As more employees have access to data that might be used to facilitate fraudulent payments activities, it is essential that businesses limit employee access to data that is not relevant to their work and ensure that employees with access to sensitive data have a record indicating that such access is appropriate and that these employees are appropriately trained to handle such data.

2.14 Processing and Dollar Volume Limitations and Associated Monitoring – Initial and Ongoing Requirement: Sponsors must set limits on each Third Party that reflect the nature of the risk associated with its business, the maturity of its processes, its capital resources, and other relevant factors. All Sponsors must set dollar limits on the maximum amount that each Third Party is allowed to process per settlement date. Effective procedures must be in place for Sponsors to monitor Third Party limits and for Third Parties to monitor limits on each entity for which it processes on a timely basis.

Rationale: These limits reflect good, basic risk-mitigation practice. The objective is to enable monitoring in a timeframe short enough to limit additional fraudulent activity. The recommendation provides for considerable implementation flexibility.

3.0 High Risk Payments Recommendations

High Risk organizations/transactions represent a special segment of the payments business that requires extended knowledge, skill, and procedures to administer. Inadequate controls and administration create significant risks to any Network and can increase cross-channel related risks among Networks. Failure to address High Risk organization-related risks could undermine consumer confidence and threaten Internet commerce. Addressing these risks will enable a more effective competitive environment for all stakeholders and will result in increased efficiencies in the payment system. The following recommendations are designed to achieve the goals of enhancing a safe, sound, pro-competitive, efficient, and consumer-friendly form of commerce.

3.1 High Risk Definition: High Risk relationships represent increased reputation, credit, strategic, liquidity, and transaction risk. High Risk entities include companies with one or more of the following characteristics:

- Historical association with criminal elements
- Difficult authentication characteristics, particularly in Internet circumstances
- Historically high rate of returns or disputes

- Poor credit or difficult to verify creditworthiness
- Reputation or compliance risk associated with the business

Illustrations include (but are not limited to):

- *Difficult authentication* (particularly in Internet context) - Includes transactions that are originated or initiated via the Internet, telephone, mail order, or by online payment processors.
- *Historical association with criminal elements* - Includes gambling/gaming, adult entertainment and tobacco.
- *Historical high rate of returns or disputes* - Includes entities such as credit repair services and online payment processors
- *Historically high credit risk, difficult to verify creditworthiness* - Includes offshore payment processors, start-up companies, and debit origination with direct access to Operator
- *Reputation and Compliance Risk* - Includes adult entertainment, gambling/gaming, offshore payment processors, and ATM/POS independent sales organizations (ISOs). Includes entities which experience or have experienced a relevant crime or non-compliance event. Includes companies associated with terrorism, or with certain foreign entities. Includes money services and foreign remittance services.

3.2 Uniform Identification of High Risk Business Characteristics: Each Network should establish a definition of High Risk merchants based upon general criteria that are common to all Networks. The precise definition of High Risk merchants may vary from Network to Network. Additional risk components to be considered before acceptance of a business falling under the definition should be identified.

Rationale: Extra due diligence and ongoing process may materially reduce risk associated with High Risk categories, and the industry would benefit from high level consistency in its definition of this important class of stakeholders.

3.3 Authentication and Authorization Procedures - Initial and Ongoing Requirement: All Network participants must employ comprehensive Network endpoint to endpoint and customer authentication tools. Authorization and dispute procedure reviews should occur during underwriting and initial sponsorship, and on an ongoing basis.

Rationale: Verification of authorization, proof of authorization, and dispute resolution competencies are necessary to reduce legal payments risk issues and to reduce costs to Network members. This recommendation is not only important in High Risk environments, but today should be considered a base line Network requirement.

3.4 Remedial Detention of High Risk Entities within Networks - Each Network should adopt rules providing for remedial detention of High Risk entities and/or their Sponsors. Rules should include provision for rehabilitation and should be Network-specific. (Detention in one Network should not, in and of itself, imply that detention is appropriate in other Networks.)

Rationale: Implementation of a remedial detention process within each Network provides protection to members of the same Network while reducing cross channel risk to members

of other Networks. Suspending transaction processing enables risk-free research periods and provides time for rehabilitation.

3.5 Enable Networks to Void Contract If Entity Causes Undue Harm - Each Network should adopt rules providing for the ability to void contracts for long term cause or severe short term cause. Rules should include provision for rehabilitation and should be Network-specific. (Termination in one Network should not, in and of itself, imply that termination is appropriate in other Networks.)

Rationale: In situations where Sponsors and/or Third Parties have clearly acted irresponsibly and those actions have produced significant harm, termination of Sponsors and/or their third parties may be the only means to protect against further loss. This is another recommendation which, in today's environment, should be considered a base line Network principle.

3.6 Notice, Termination, and Re-Sponsoring Terminated Parties - Networks should enable an effective means of communicating appropriate information to their members whenever any party's participation in the Network has been terminated for cause.. Networks should adopt provisions for the prevention of re-sponsorship of High Risk entities for significant harm. Rules should include provision for rehabilitation and should be Network-specific.

Rationale: Implementation of Network-specific prohibition within each Network provides protection to members of the same Network and members of other Networks. Providing notice of termination reduces risk both within the Network and, in some cases (such as in gateway situations), to other Networks. Providing payment system education programs increases responsible behavior.

4.0 Information Security Recommendations

Headlines reporting breaches of payments data have become so frequent that customers are no longer surprised by these incidents, even when they occur at large, respected merchants. Increasingly, data breach incidents involve both card and check data. Recent incidents have compromised returns-related data, increasing risk to account holders and their financial institution. All stakeholders would benefit from more closely coordinated data protection requirements and enforcement regimes, perhaps built around the Payment Card Industry (PCI) security standard. The standard seeks to achieve end to end levels of security from merchant to processor to FI and, where appropriate, back to the merchant.. Suggestions for coordination follow.

4.1 Expanding PCI Requirements to Other Networks: General Statement - All Networks are encouraged to adopt data security standards modeled upon appropriately-modified versions of the PCI Data Security Standard.

Rationale: Functional convergence across payments applications has led to increasingly parallel data storage issues across payment silos. The industry would benefit from uniform data security standards, with appropriately customized modules to suit specific payment applications as required.

4.2 Expanding PCI Requirements to Other Networks: Continued Dialogue - The PCI Security Standards Council should expedite its dialogue with other electronic transaction Networks to expand adoption and to develop the standard as truly open (with an appropriately open governance model). The Council should consider inviting representatives from all key EFT systems, including the ACH, to explore whether standardizing certain PCI compliance elements might result in a more effective and efficient compliance process, to the benefit of all stakeholders.

Rationale: Leveraging an open standard that is Network level adaptable creates an opportunity to increase the security within existing data platforms, allows organizations to better manage their IT and audit investments, and provides the basis for a more successful and comprehensive approach to enterprise wide security and risk management.

4.3 Expanding PCI Requirements to Other Networks: ACH - While PCI is a good standard for data security and audit, it will require modification for implementation in the ACH. The Working Group encourages the industry to explore whether and how a common PCI compliance and enforcement regime might be established. Such a regime could be leveraged against multiple payments applications and Networks, with the goal of reducing unit costs for all stakeholders.

Rationale: Cost effective compliance and enforcement is particularly important in the ACH. Non-certification shared assessment programs such as the Financial Institution Shared Assessments Program (FISAP) suggest such regimes could be effective in this situation.

4.4 Expanding PCI Requirements to Other Networks: “Real Time” EFT Networks - Real time EFT Networks are encouraged to adopt an appropriately-modified version of the PCI Data Security Standard. The standard should be modified to include additional provisions to incorporate requirements relating to the protection of symmetric keys and PINs. These issues would need to be addressed before PCI could become a standard for Real Time EFT Networks.

Rationale: The industry would benefit from common data security standards and a compliance process that, wherever possible, has been honed to achieve maximum effectiveness and efficiency. The PCI standard’s current scope does not appropriately encompass symmetric keys and PINs.

4.5 Regular Security Reviews of Third Parties - Sponsors should perform security audits of Third Parties with which they have a contract. Security audits should generally be performed on an annual basis, but may be performed more or less frequently on a risk-adjusted basis. Each Network should:

- Create thresholds that are pertinent to the Network’s business sector to define entities that can self assess and entities that must enlist the services of an independent Third Party assessor.
- Provide standards and audit guides for both the self assessments and the independent assessments.

- Clearly define within each Network's rules the potential protections and penalties should an issue occur within an environment that did not adhere to this Network rule.
- Define timelines for compliance that encourage adoption while allowing entities to appropriately prepare and execute accurately in the event that immediate adoption within a particular Network proves to be challenging.

Rationale: Regular information security audits of Third Parties are essential to ensure consumer confidence and limit risk.

4.6 Cross-Network Notification of Security Breaches - In situations where there is a suspected breach of security, a Network should promptly notify its members, and Network members are encouraged to:

- Conduct internal investigations to ensure that breaches have not occurred in other channels.
- Evaluate how the compromised data could present vulnerabilities within other payment platforms.

If compromises and/or vulnerabilities exist across multiple channels, all affected channels should be notified.

Rationale: Increased convergence of payments system functionality has outpaced the ability of financial institution sponsors to monitor all small value payments Networks comprehensively.