

THE PARTNER GROUP

LIABILITY FLOWS AMONG NETWORKS COMMENT LETTER ON CROSS-NETWORK LIABILITY FINAL

ABOUT THE PARTNER GROUP

The Partner Group is an informal work 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
- Third Party Payments System Access Control Working Group
- Liability Flows Among Networks 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 jump the tracks between small value (retail) payments transactions. The Working Group's purpose is to develop improved fraud reduction information-sharing capabilities among payments networks in different silos. The Group's initial focus is on merchant data bases. This work team is co-chaired by Glen Sgambati, Chief Data Officer, Early Warning Services LLC; and Ward Gailey, Senior Vice President, SunTrust.

ABOUT THE THIRD PARTY PAYMENTS SYSTEM ACCESS CONTROL WORKING GROUP

The Third Party Payments System Access Control Working Group was formed to develop common processes and standards, as appropriate, relating to third parties—merchants, Independent Sales Organizations (ISOs), third party entrants, etc.—for payments system access control. The Working Group is initially focusing on ISOs and third party entrants. The Working 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 Policy, ICBA; and Lou Anne Alexander, Senior Vice President, Wachovia.

ABOUT THE LIABILITY FLOWS AMONG NETWORKS WORKING GROUP

The Liability Flows Among Networks 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 and language for "strawman" operating rules 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. In addition to the co-chairs, the Liability Flows Among Networks Working Group's current membership includes:

- Joseph R. Alexander, EPN
- Debbie Ashley, Washington Mutual
- Doug Balough, Wells Fargo
- Tom Barnett, Wachovia
- Donna Carbone, Bank of America
- Martin Elliott, VISA
- Jeanette Fox, NACHA
- Ian Macoy, NACHA
- Dan Miner, NACHA
- Dennis Simmons, SWACHA
- Trish Lancaster, NYCE – Metavante
- Jeffrey R. Tansill, BB&T
- David Van Horn, VISA
- Bobby Whisenant, Compass
- John Yanish, FRB Minneapolis
- Susan Zawodniak, NYCE

This project was managed by The Santa Fe Group on behalf of BITS. Funding was provided by a group of BITS member financial institutions. Tom Hemnes 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.

LIABILITY FLOWS AMONG NETWORKS WORKING GROUP PROBLEM DEFINITION

Compromise and misuse of customer payment data (e.g., card or account number, authentication values) is a risk of concern to all participants in the payments industry. When fraudulent transactions result from a compromise and misuse of payment data, the financial institution whose customers and accounts were impacted suffers financial losses, loss of consumer confidence, remediation expense, and reputation loss.

To ensure that participants in the payments industry take responsibility for protecting customer payments data, it is important that entities which allow data to be compromised are held responsible for the misuse of that data. It is also important that there be a clear liability path for fraudulent transactions resulting from data compromise, even when the data compromise and data misuse occur in differing payments networks.

In the US financial services industry, it is common for financial institutions to participate in multiple electronic payments networks based on products and services, geographic reach, service, pricing, and other network characteristics. Financial institution customers initiate payments using various access devices (e.g., card, chip, check, account number) and channels (ATM, POS, Internet, VRU), and those payments are routed through one and sometimes multiple payments networks for processing. Historically it was not uncommon for institutions to participate in one signature debit network and four or more PIN debit networks based on the region(s) in which their ATMs were located or cards issued, the products they needed (ATM, PIN POS), and historical ownership of the regional PIN debit networks. Over time, regional networks have merged to cover a large portion of the US. Today it is rare for any financial institution to participate in every US-based PIN debit network. Rather, financial institutions generally participate in one or two US-based PIN debit networks in addition to an international PIN debit network.

When a data compromise occurs, and the data is misused to perform fraudulent transactions, the impacted institution may seek restitution from the payments network participant which allowed the compromise to occur. The network's process for seeking restitution is outlined in its network rules, and all participants in the network agree to abide by the established process.

Because financial institutions often participate in multiple payments networks, it is possible for a situation to arise in which a data compromise occurs at an entity within one payments network and the compromised data is then misused in a second payments network. For example, the data related to a legitimate point of sale transaction might be compromised at an entity which participates in PIN debit network "A," and the compromised data used to initiate a fraudulent transaction at an ATM participating in network "B." Today, in these situations, there is no clear and consistent process through which an impacted institution can seek restitution when the data compromise and fraudulent transactions occurred in different networks under different rule structures.

There is no clear channel of recovery across networks. Even networks with the broadest indemnity rules indemnify only their own members. Furthermore, the law generally provides no means of recovery because of the "pure economic loss" rule of torts law and the fact that there is usually an intervening actor (the bad guy) who proximately causes the harm.

A clear, comprehensive process for addressing loss recovery is necessary for card issuers, transaction acquirers, and payment networks. Card issuing financial institutions need to have a method for recovering fraud losses occurring as a result of another network participant's actions, and need to be confident that a rules loop hole will not result in the card issuers having no recovery options because they participate in multiple networks. Transaction acquirers—both the sponsoring financial institution and merchant—need to have clear rules establishing compliance obligations, transaction liability determination, and limitations on liability. Only with clear rules can an acquirer understand and quantify compliance risk and liability. And, finally, payment networks need to exist in an environment where institutions are free to choose participation in any network which provides the competitive products and services they need without being penalized when they attempt to recover losses for transactions which occur in a network other than where the data was compromised. This document describes a series of alternatives for addressing the need for inter-network, and cross network, liability flows.

The Liability Flows Among Networks Working Group sought comments on both the problem statement outlined above and the range of proposed solutions suggested below. Comments were accepted until the close of business, January 29, 2007. Comments were considered by the Working Group and incorporated into the document. Recommendations are directed primarily to card networks. Work is underway in the Risk Management Advisory Group at NACHA as well as in other venues that will suggest whether and how the ACH should be addressed in additional recommendations. Additional work may also address such issues as establishing standards for recoverable costs.

HIGH LEVEL SUMMARY OF PROPOSED SOLUTIONS AND RESPONSES

Support for several approaches to proposed solutions that were identified by the Working Group suggests that additional effort to further hone these approaches is appropriate. Some networks are actively pursuing related programs. The most widespread support was expressed for a shared forensic approach to investigating security breaches and other fraud-related payments events. It has become clear that there is significant duplicative process today. In some instances, a lack of cross-network cooperation is causing a delayed remedial response. Insurance programs tied to security audits are under consideration by some networks. Many comments suggested that issuers should meet a threshold level of practice in protecting customers against security or fraud threats in order to make claims using any of the proposed solutions outlined below. Descriptions of these proposed solutions, with pros and cons for each, are outlined in the sections which follow.

POTENTIAL SOLUTIONS TO THE PROBLEM

Proposal for an Insurance Pool

One possible solution considered by the Partner Group would be the creation of an industry-wide insurance pool. The theory underlying the creation of such a pool is that security and data breaches are a predictable occurrence, the risk of which can be most efficiently spread and protected against if it is shared by all members of the industry. The alternative of attempting to allocate loss to the industry member responsible for the security breach is, arguably, less desirable, for at least two reasons. First, there is a high transaction cost in attempting to assign blame, and persons accused of security breaches are likely to resist the allegation forcefully. Second, the persons responsible may not have sufficient resources to pay the losses of the industry as a whole in the event of a serious security breach.

The pool would work as follows. All participants in the payments industry might be required to pay premiums into the pool. The amount paid by each participant would be graduated according to the effectiveness of that participant's risk-mitigation tools and practices, as well as the results of compliance reviews. Participants with more effective risk mitigation would pay less than others which posed a higher risk. This approach would provide an incentive for payments system participants to put effective security measures in place.

Pool members would, of course, be required to maintain appropriate minimum levels of security to gain the benefit of the insurance protection and would be subject to audit by representatives of the insurance pool. The industry would have to agree generally to common security standards across payments networks. Some security standards, such as PCI, have already shown promise and effectiveness in ensuring that appropriate security practices are observed among payments system participants. The BITS Third Party Access Control Working Group is developing a Maturity Model Framework which could also be used in conjunction with the PCI standards to grade the risk posed by individual participants (the Maturity Model addresses complementary issues to those addressed by the PCI standards).

In the event of a loss, the industry members suffering the loss (typically issuers) would be entitled to recover the loss directly from the pool (subject to appropriate reserved amounts and liability caps). There would be no claim directly against the acquirer or merchant who was responsible for the loss, but, in cases of repeated or grave failures, that entity's participation in the payments networks could be terminated.

Advantages to an Insurance Pool Approach:

Such a scheme has the advantages of certainty and efficiency of recovery. It also presents a clear funding model when compared to other solutions, and incorporates a funding model that encourages desired behaviors.

Disadvantages to an Insurance Pool Approach:

The approach might require the establishment of an entirely new entity—the mutual insurance pool—and of obtaining industry-wide buy-in for the creation of such an entity. Alternatively, an existing organization, such as the PCI Security Standards Council, could be used in an industry-wide approach. Some large, well-capitalized financial institutions may feel the approach is unnecessary, since they are highly solvent and in a position to self-insure. Also, unless carefully implemented, it has the disadvantage generally associated with insurance solutions, which is to dilute the risk of direct responsibility for negligent behavior, while in effect taxing some entities with security systems good enough to avoid the harm caused by firms with inferior security behaviors. In many other situations (professional liability insurance, errors and omissions policies, etc.) these negatives are, however, overcome by the substantial benefits insurance schemes provide for industry players as a whole. Additional challenges remain, such as solutions to the following questions:

- If funds are inadequate to cover losses, on what basis would payments be issued?
- Would institutions that have not paid into the pool be eligible for funding? If not, could they take legal action?
- Would distribution be pro-rata based on contributions to the fund or some other common denominator, such as asset size?

Proposal for a Common Indemnification Approach

Another proposal considered by the Working Group is for networks to adopt an indemnification approach whereby members of each network agree to indemnify members of their own network and of other networks for losses arising from network rules violations, violations of law, and/or violation of the rules/requirements of any other network to which transactions are routed by the original network. This approach assumes that any network adopting this approach would maintain rule sets that effectively address threshold level security and confidentiality obligations.

This approach provides a contractual mechanism by which all members agree to indemnify the networks and network members for a defined class of acts/omissions. The industry would establish procedures and limits for liability in situations of catastrophic loss. A framework would be established to ensure that smaller networks bear an appropriate burden of the costs of such an approach, and that larger networks do not carry a disproportionately large load.

The industry would also have to agree on additional caps on liability, as well as caps on recovery, based on the circumstances of security breaches, and the associated risk-mitigation tools in place at the time of the breach. A time frame for recovering losses after a breach would also be established.

Advantages to an Indemnification Approach:

This approach provides an avenue to recover damages for breach of network rules from a party with which it otherwise has no privity of contract. Network

resources are not required to address or adjudicate disputes. The incentive for each network member to control access to sensitive information is maximized.

The possibility for negative publicity that could result if a claimant filed litigation to have its claim adjudicated—and the expense—would likely be an incentive for the parties to settle the dispute informally and not resort to litigation.

Networks may feel that stand-alone indemnification policies are effective competitive differentiators that suffice to provide recovery for losses caused by security breaches, and historically that view is correct. However, The Partner Group believes that there may now be definable circumstances where the potential risks to the payments industry as a whole would seem to outweigh the value of differences in indemnification approaches as competitive tools.

The industry has already experienced events which, if repeated with any regularity, would rise to this level. The first quarter of 2006 saw a major PIN debit compromise through which large numbers of customers were defrauded in an attack of unprecedented size in the PIN debit arena. Major EFT networks believe this attack met the criteria where a compromise in one network affected customers and financial institutions in another. Attacks of this type, should they occur on a frequent basis, clearly have the ability to harm consumer confidence and impact consumer behavior. Even without that behavior change, attacks of this nature may significantly decrease the operating efficiency of card networks, to the harm of all stakeholders, including end user customers.

Disadvantages to an Indemnification Approach:

Recovery through an indemnification process may be costly and time-consuming if the contractual obligations were disputed, and some arbitration process between networks would be likely. There is no guarantee that the indemnifying party will have sufficient financial resources to cover the loss suffered, despite the fact that networks typically require financial institution sponsors to be liable for non-financial institution participants in the network. Therefore, even if a financial institution sponsor “stands behind” and indemnifies other parties against loss, the concern of financial adequacy of the sponsor remains, in the event of significant losses due to fraud.

Also, for this approach to be successfully adopted across networks with different business models, limits on the scope of any cross-indemnification would be required. It remains to be seen if those limitations would be so great as to defeat the intent of the approach.

Proposal for an Indemnification Approach Extending Existing Network Process and Rules

A variation on a common indemnity approach was also discussed by the Working Group. In the proposed alternative approach, each network would open its

existing claim resolution process and indemnification structure to participants in its network to include suspect transactions processed outside of the network provided that the: 1) original data compromise occurred within the network; and 2) other networks reciprocated. In effect, a network would simply extend its existing process and indemnification policies resulting from suspected compromise within its network to transactions which were processed in another network if that other network did the same thing. This approach would require a common set of security standards across networks in order to operate effectively. Indeed, the Working Group received comments suggesting that the defined class of acts and omissions and scope should include:

- Storing and sharing of account numbers or any customer information not authorized by network rules
- Growing penalties for repeat offenders and non-compliance with network standards
- Guidelines for on-site audit reviews
- Network reporting requirements

The approach would provide an avenue for some recovery, subject to whatever limitations, burdens of proof, etc., the networks already have in place.

Advantages to Indemnification Extending Existing Process and Rules:

This approach requires minimal change in existing network rules and processes. It addresses the problem of inter-network loss while retaining each network's ability to establish its own rules for liability, thus preserving competition on this aspect of network function. Finally, it does not require the creation of new and innovative procedures or facilities.

Disadvantages to Indemnification Extending Existing Process and Rules:

Recovery for loss and procedures for recovery will not be uniform across networks. Further, some networks may choose to provide minimal recovery in all cases, which would compromise the benefits of the plan.

Proposal for Third Party Arbitration

Another approach being considered to address the problem is the establishment of a third party arbitration process for resolving cases involving multiple networks. This approach assumes that an independent third party is agreed to by all of the participating payments networks, that the third party is provided copies of each of the participating networks operating rules, and that the third party is briefed in detail on the network's arbitration and grievance process related to fraud losses incurred as a result of a data compromise. The payments networks would also agree to have restitution claims involving transactions spanning multiple networks be referred to the independent third party. This approach assumes that the payments networks would modify their operating rules to provide for the use of a third party arbitrator to resolve an inter-network claim. The financial institution requesting restitution would provide the third party arbitrator with

information related to the fraudulent transactions and the information which the institution has which implicates the entity they believe allowed the compromise. The entity which is accused of allowing the data compromise would provide the third party with whatever evidence, forensic or otherwise, that responds to the complaint. The third party arbitrator would review the evidence and respond with an opinion as to liability and restitution requirements, if applicable.

Advantages to Third Party Arbitration Approach:

A third party arbitrator, independent of the payments networks, would serve as an independent mediator in reviewing the fraud loss claim and verifying that the fraudulent payments which occurred in one network coincided with the card or accounts compromised in the other network. The third party arbitrator would be familiar with the relevant network rules and agreements for all of the impacted participants and would be in a position to give consistent results over time based on a standard, agreed-upon process. The independent third party arbitrator would also bring the advantage of eliminating any network-specific bias towards a particular customer and ensure equal treatment for all claimants. Finally, having a third party arbitrator review the records from the impacted institution(s) would eliminate the need for the network(s) to manage complex inter-network compliance cases.

Disadvantages to Third Party Arbitration Approach:

Because liability for fraudulent transactions will continue to remain with the entity which allowed the compromise to occur, it is uncertain if this solution provides much benefit other than to add an additional participant and layer of complexity to the arbitration process. It would require educating an entity outside the industry on a very complex web of network rules and contracts that are difficult even for industry insiders to understand. It would not establish legal precedents regarding liability flows between networks, nor would it provide ability for any of the involved parties to appeal the arbitrator's decision. It would require that sensitive customer and internal data be provided to a third party with which the institution or entity does not have a business relationship. Information provided by the entity accused of the data compromised would not be available to the network or the impacted institution, limiting the ability of the network to take further action to reduce risk for other network participants and hampering the impacted institution's ability to prove its claim. Finally, using a third party arbitrator would increase the cost burden of managing arbitration cases.

Proposal for Shared Forensic Investigations Approach

There appears to be significant industry support for a shared forensic approach if carefully and appropriately crafted. This approach could require—potentially via new or amended network rules—that a compromised entity, or the financial institution that is a member of one of the partner networks, engage a Qualified Incident Response Company (QIRC) to perform a forensic investigation. Ideally, each participating network would adopt this rule.

The results of the investigation could be shared with all impacted networks, alleviating the need for multiple separate forensics investigations. Forensic results would be shared directly among networks, which would control distribution to their members. This would also have the effect of reducing the costs of investigations, which are often conducted independently by multiple networks. New or revised rules would stipulate that the results from a forensic analysis would be used as the primary basis for determining whether and how a network's rules had been violated and for establishing responsibility for any losses incurred.

The following actions could be included as part of the forensic investigation:

- Perform incident validation and assessment.
 - Establish how the compromise occurred.
 - Identify the source of the compromise.
 - Determine timeframe of the compromise.
 - Review the entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production systems, as well as VPN, modem, DSL and cable modem connections, and any third-party connections.
- Determine if the compromise has been contained.
- Create an incident report with:
 - An executive summary of findings
 - General information about the company being investigated
 - Their status with respect to Payment Card Industry Data Security Standards
- In addition to the above, for compromises involving subsequent PIN fraud, a PIN security review should be done as part of the forensics to evaluate compliance with PCI PIN security requirements.

Other general forensics considerations:

- Objective criteria should be established to qualify vendors that will be accepted for forensics.
- Consideration could be given to proposing the criteria be added to Payment Card Industry Data Security Standards (PCI DSS) which could then be managed by the new PCI Security Standards Council.
- Each network would be responsible for enforcement since participants in networks would, presumably, be bound via their network rules.

Key barriers to the implementation of this approach are privacy restrictions that currently exist in network rules, contracts and statutes, and concerns about liability claims if information about a transgressor turns out not to be true. The industry would need to find a way to share sensitive information without compromising privacy concerns, and to deal with liability claims.

If a PCI certification were done at the suspected source of the breach, the team doing the forensics investigation should be different than the one that certified them as PCI compliant.

The Working Group received comments suggesting the need for a business case to ensure that process efficiencies would accrue as expected. Comments suggested that the business case should address the following issues:

- A process must be agreed upon to identify third parties who would conduct the investigations.
- A decision is required on whether the claimant or the defendant will absorb or share the cost of said investigations.
- A defined minimum threshold or floor limit needs to be agreed upon by all parties.
- A common investigative output has to be standardized and agreed upon by all parties.
- The deliverable needs to be acceptable as concrete, irrefutable evidence that may be used by a court of law or third party arbitrator in the ruling.

If it is determined that this forensics approach is one that should be adopted by the industry on a broad basis, then an institution will need to be identified to determine a framework to guide QIRC investigations. Also, common agreements for the use and sharing of confidential information relating to customers and transactions would have to be agreed upon by participating networks and their member financial institutions. Qualified institutions may include BITS, EFTA or the PCI Security Standards Council, among others.

Advantages of the Forensics Approach:

This is a reasonably thorough approach and forensics can often pinpoint the problem source.

Disadvantages of the Forensics Approach:

Liability may not be established even if fault is determined. This approach may be expensive for some payment networks. Implementation would require changes in network rules or other means of requiring participants to abide by the approach.

For Additional information about The Partner Group, and this Liability Flows Among Networks Comment Letter, contact either Matt Ribe, BITS Project Manager, matt@fsround.org; or Gary Roboff, BITS Senior Consultant, gary@fsround.org.