POLICY STUDIES

Legal Analysis of a Banking Industry Online Identity and Attribute Authentification Service for Consumers and Merchants: The Financial Service Technology Consortium's FAST Initiative

William Gram
Federal Reserve Bank of Chicago

Emerging Payments Occasional Paper Series
September 2000 (EPS-2000-2)

FEDERAL RESERVE BANK
OF CHICAGO

ABSTRACT

This is a legal and risk analysis of an online identity and attribute authentication service developed by the Financial Agent Secure Transaction (FAST) initiative of the Financial Service Technology Consortium (FSTC). The FSTC is a not-for-profit group organized to enhance the competitiveness of the financial services industry. Members include banks, financial services providers, research laboratories, universities, technology companies and government agencies. FSTC sponsors project-oriented, collaborative research and development on inter-bank technical projects affecting the financial services industry. A complete report on the FAST initiative will be available to FSTC members in September 2000 and to the general public by late 2000. Contact the American Bankers Association web site at that time to download the paper or contact the writer at the email address below.

During the FAST initiative, the author was the leader of the FAST Legal/Risk Workgroup. This paper is primarily the author' s product with input from Patricia Allouise of the Federal Reserve Bank of Boston and Ann Spiotto of the Federal Reserve Bank of Chicago. The views expressed in this report are solely the writer' s and do not necessarily reflect the views of any component of the Federal Reserve System or the Federal Reserve Bank of Chicago, the writer' s employer. This report is written at a very general level and is designed to highlight issues and problems rather than give legal advice. The reader is advised to consult expert legal counsel before taking any action related to the views expressed in this report. The report addresses the following questions: (1) What is FAST and how does it work? (2) What are the legal risks and how might they be handled?

The Occasional Paper Series is part of the Federal Reserve Bank of Chicago' s Public Policy Studies series. This series includes papers on various policy issues that are generally less technical and more appropriate for a wider audience than working papers. These papers may not go through as extensive of a review processes as associated with some academic journals in the interest of sharing information and analysis on a more timely basis.

Address any correspondence about this paper to William Gram, Federal Reserve Bank of Chicago, 230 South LaSalle Street, Chicago, Illinois 60604 or e-mail Bill at william.gram@chi.frb.org. Requests for additional copies should be directed to the Public Information Center, Federal Reserve Bank of Chicago, P.O. Box 834, Chicago, Illinois 60690-0834, or telephone (312) 322-5111.

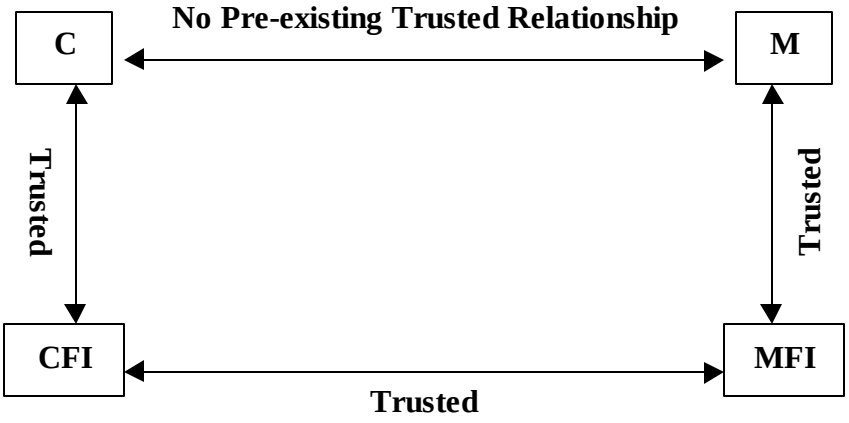
TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

In a basic FAST transaction, there would be four participants:

- Two financial institutions (FI' s) that are known to each other and have a trusted relationship with each other evidenced by a contract; and
- Two customers that have no trusted contractual relationship with each other but each has a trusted relationship with its FI evidenced by a contract.

In a FAST consumer (C) Internet purchase transaction with a merchant (M), each would use its trusted contractual relationship and secure Internet connection with its FI (CFI or MFI) to forward identity and attribute (I/A) information to the C or M as required by the transaction. In essence, the customers and FI' s use the web of trusted contractual relationships to obtain the trusted information necessary to go ahead with the transaction. That network is depicted below:



FAST is envisioned as a private (members only) online system run by financial institutions to create, hold, transfer and vouch for a standard set of identity and attribute information. It builds on the existing trusted contractual relationships and online security connections between FI' s and their customers. An attribute might be "age 21 or over", "authority to bind X corporation", "domiciled in X state", social security number etc. In FAST, it is defined as an item of information about a customer that is tied to his/her identity. Identity, for purposes of FAST, is evidence that a customer is in fact the customer. It is established by various methods, including checking identification documents like drivers' licenses and social security cards. Financial institutions (FI's) will collect this information from customers and store it to be used in later FAST transactions. This may be collected when the customer opens an account or it may be collected later.[1] In a FAST transaction, a FAST enabled customer will use it' s online banking connection and security password to request that one or more of the (I/As) held at it' s FI, be issued and forwarded to another FAST enabled customer, to facilitate an online transaction. The actual transaction will involve the other customer' s FI. When the request is received, the issuing

[1] A major issue for FAST is the accuracy of information that was originally collected to open a standard bank account, perhaps online, but that will now be used in FAST transactions.

customer' s FI (CFI in the example) will vouch for or warrant the accuracy of the I/A information and respond to the request online to the FI of the relying party (MFI in the example). The relying party' s FI will, in turn, transfer and warrant the I/A information to its customer, the relying party (M in the example). Transfers may or may not include payment or payment information. The FAST technology approach is depicted in the four corner model above, with the FAST management organization acting as a fifth participant by facilitating and storing transaction information in a database that exists between the two FI' s. This structure will probably be governed by FAST minimum standard contracts and operating rules between the management organization and the FAST FI' s on the one hand, and the FI' s and their customers on the other. In short, FAST will be a private contractual system for FAST FI' s and FAST enabled customers only.

While there are several possible ways to structure FAST, this report will focus on a warranty approach. The reader should note that the approaches described in this report assume that the rules and contracts will be enforceable and will act as designed. This may not always be the case. Some of this risk is discussed later in the report. Under the contracts and rules, FI' s may agree to warrant the accuracy of the I/A data to each other and to their customers. If this approach is adopted and there is an error, a customer' s only recourse under the rules would be to its FI, which warranted the data to the customer. In turn the FI' s only recourse would be to the FI that warranted the information to it. All other FAST FI' s and the management organization would be isolated from liability by the FAST web of private contracts and rules provided, of course, they work as designed. Strong liability limitation provisions could be included in FAST contracts to limit a FI' s liability to relying parties, other FAST FI' s and non-FAST third parties. The report considers tort, contract and other legal liability risk. The fact that a FAST transaction, as presently envisioned, will often only produce an answer to an I/A question and that may consist of a yes or no to the customer, is a distinguishing feature of FAST. Unlike an accountant or financial advisory statement, or a digital certificate, a FAST transaction should not result in a document that a non-FAST third-party can read and rely on. Furthermore, FAST rules and contracts could be drafted to bar a customer from forwarding FAST transaction information to others, as well as limit the amount a customer could recover for a FI' s error. In theory, this could limit third-party legal actions that might involve a FAST FI. On the downside, it could also limit customer interest in becoming part of FAST and paying FAST fees. The report ends with sections on the regulatory environment, risks not discussed in the liability section and suggestions for managing FAST risk.

Following are some of the more important issues and risks raised in the report:

1. Negligent Misrepresentation Tort Risk - FAST FI' s could be subject to liability in forwarding an erroneous identity or attribute. See Section 3.3.

2. Fair Credit Reporting Act - FAST FI' s and other FAST participants could be subject to the act depending on how its language is interpreted. See Section 4.1.4.

3. Patent Infringement - There may be patents on the business methods and software that will be used in FAST. See Section 3.6.1.

4. FAST FI' s As Third Party Defendants - Can FAST FI' s be insulated from open-ended liability when a relying party such as a merchant is sued for an identity or attribute mistake? See Sections 3.4.1 and 3.4.2.

5. FAST Adoption - Will the FAST product be adopted by relying parties such as merchants if the FI' s limit their liability for mistakes?

6. Liability Limitation - Can liability limitation clauses in FAST contracts be effectively implemented, especially in the consumer arena? See Section 3.4.1.

7. Third Party Lawsuits - Can third parties pierce the liability limitation structure to recover from FAST FI' s? See Section 3.4.2.

8. There may be trademarks on the word FAST. See Section 3.6.4.

9. FAST FI' s may want to offer the option of purchased insurance as VeriSign does to reduce merchant risk. See Sections 3.4.1 and 3.4.2.

2 WHAT IS FAST AND HOW DOES IT WORK?

The FAST project in Phase One consists of studies by several workgroups followed by a white paper report at the end of six months. The initial workgroups reported on similar initiatives in the marketplace or in development. A chart of business requirements and needs was created. Three detailed fact scenarios called "use cases" were developed to test both the business requirements and the FAST "solutions" developed by the technical/functional workgroup. Use Case One detailed the FAST role in a consumer purchase from an online domestic wine merchant. Use Case Two described a trading partner exchange and Use Case Three defined the FAST role in an employment eligibility scenario. The FAST leadership in Phase One decided to focus primarily on Use Case One.

2.1 THE MANAGEMENT ORGANIZATION (MO)

The FAST structure needs to be created and organized. In membership or common interest organizations, a separate legal entity, often a limited liability company (LLC), is established as a separate legal entity to limit the risk to the membership organizations.

For purposes of this paper it will be called Management Organization (MO). It would be responsible for a number of activities:

1. MO could be established by a subgroup of FAST FI' s that would be equity or governing members of MO. In theory, MO could be established by non-FI' s or an existing rules group. For purposes of discussion, this paper will assume it is established by a subgroup of FI' s, which contribute the capital necessary to establish MO.

2. MO will be responsible for developing the standards, rules, software and structure of a FAST technology solution. At the core of the solution is a database and related software, housing references to all participants, as well as, information referring to customers that have had transactions processed. The technology solution does not exist in any one location but instead consists of a set of software containing access control to the database etc, as well as support for FI customers and FI legacy interfaces. The MO technology solution will also be responsible for assuring that FAST FI participants can communicate with other participants and deal with problem situations.

   FI access to the technical solution database can take two forms. If the FI will be running its own technical solution within FAST, it will need its own MO technical solution database and a software agent to operate it. If, instead, a FI opts not to operate its own database etc, it will contract with an MO approved Application Service Provider (ASP), which will provide the FI' s with interfaces to the MO database etc. Thus, the MO database and associated software is not housed in any one location but instead is distributed among FAST FI' s and the ASP.

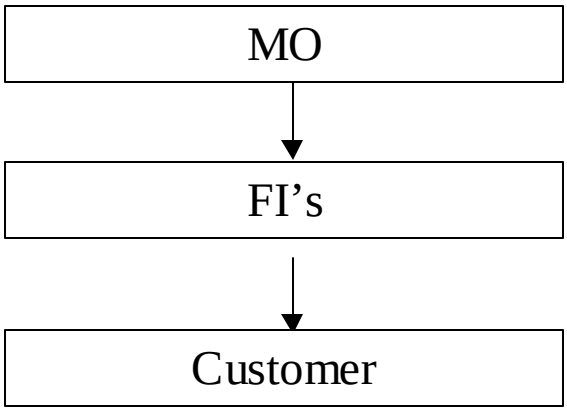
3. MO establishes the minimum standards, rules, etc. governing the FI/MO relationship and enters into the FAST contract that enrolls the FI as a FAST member.

4. It also handles the FAST dealings with the MO approved ASP described in 2.

5. MO establishes the minimum standards, rules, contract terms etc. for the relationship between a FAST FI and its FAST enabled customer so there is interoperability and a common approach. In the example above, this would most probably consist of an add-on to the FI' s existing banking contract with C and an addition to an FI' s existing contract with M.

The FAST goal of working with the existing infrastructure between FI' s on the one hand and between FI' s and their customers on the other, means that MO will attempt to keep its rules and standards as minimal as possible while still meeting the FAST overall goals. At the FI level, this will mean a MO contract with simple rules governing the FI duties and responsibilities. At the customer level, there will be no MO contract with customers. Instead the FI' s banking contract with its customers will most probably be the means used to bring in the FAST contractual terms.

The MO authority structure would look like this:



A prior version of this technical solution made use of a centralized database and switch operated by an entity called FASTCO. In the current version, there is no switch, no centralized database, no FASTCO. The current technical solution is a distributed database and related software. While FASTCO is gone there is still a need for a minimal central authority. Even if most of FAST is outsourced to an experienced rules organization, there may still be a need to provide oversight and deal with liability through a separate entity. In this paper, MO is running the technical solution and other central or common activities. These could be broken up into parts, outsourced and run by one or more other organizations. However, for purposes of this analysis, it is assumed MO is the central operating authority.

2.2 ONLINE CONSUMER PURCHASE FROM MERCHANT – USE CASE ONE

2.2.1 Assumptions

The typical FAST transaction assumes two FI customers, C and M, are involved in an Internet transaction and are unknown to each other (no pre-existing trusted relationship). Each FI:

1. Has a trusted relationship with its customers;

2. Is a FAST member bound by a contract with MO;

3. Has FAST minimum standards contractual provisions in its banking contract with C or its merchant contract with M;

4. Is FAST-enabled and has some sort of electronic banking connection with its customers so FAST identity/attributes and possibly payments can be transacted electronically. At the M level, there will be a server agent (software) provided by MFI that will assign participant and transaction IDs and support interactions with the technical solution database. This agent may also support C access to FAST services or support a C electronic wallet;

5. Has its own security mechanism in place to authenticate that its customer' s message came from its customer (identity authentication); and

6. Has certain standardized attribute information about its customer, which can be transmitted with customer permission during a FAST transaction (for example, age 21 or older, state of residence, existence of a demand deposit account, merchant rating information, etc.), which the FI is willing to stand behind.

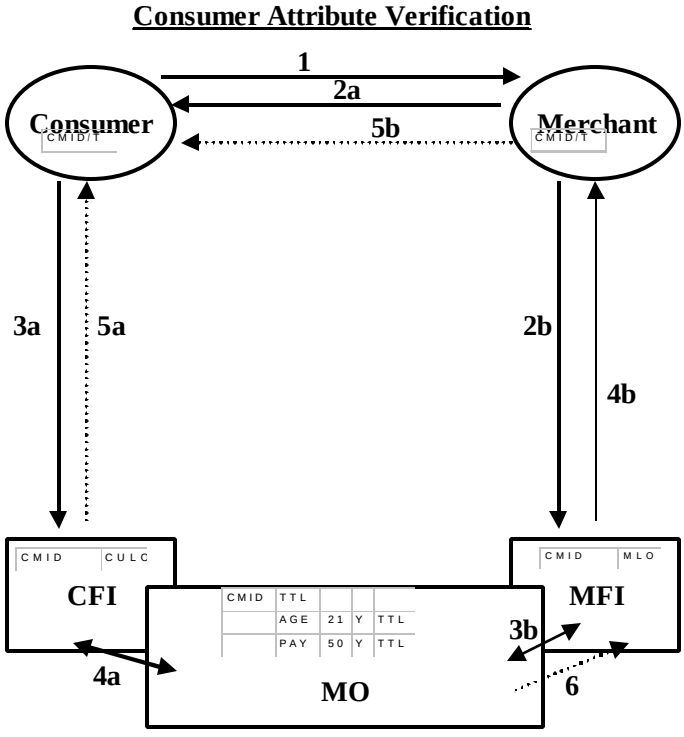
2.2.2 Issuing And Relying Parties

In a FAST consumer/merchant transaction either party can ask for I/A verification. The consumer might want to verify that the web site is really M' s. C would use FAST to verify M' s identity and perhaps other business-related attributes. In this case, M, through its MFI would issue the information. Here M would be the issuing party and MFI would be the issuing party FI. C would be the relying party since it requested the attribute verification and is relying on it in the

Internet transaction. CFI is the relying party FI. These roles are reversed when M uses FAST to request an identity and attribute verification from C, such as age 21 or over. Here C would be the issuing party and M the relying party. M wants this information before it proceeds. CFI would be the issuing party FI and MFI would be the relying party FI. These designations have significance because the FAST legal rules on liability, claims handling and dispute resolutions, etc. may be written in terms of issuing parties and relying parties. This will be discussed later in this paper.

2.2.3 Steps When M Requests An I/A Verification From C

The core of the current FAST technology solution is the MFI provided software agent located on M' s server. M receives this when it enrolls in FAST. While C has agreed to a CFI electronic banking contract, which includes FAST contractual terms (this constitutes FAST enrollment), it is not necessary for C to download or install any special software to participate in FAST. The standard Internet browsers resident on most computers will handle it. (This also facilitates expansion of this service to the wireless arena.) When C submits its purchase order to M and M requests permission to obtain an age verification which C grants, the software agent on M' s web server creates a unique ID and I/A request and forwards it in two directions at once to C (who forwards it to CFI) and to MFI. The two attribute request ID' s then meet again in the MO database where CFI' s answer to the request is picked up by MFI and forwarded back to M. The graphic and steps for this follows:



Step 1 C Grants M Approval To Verify Attributes

C engages in a shopping experience with M' s web site, completes a purchase order and hits the submit button.

M needs an attribute verification on C, for instances, age 21 or over (It is one of a limited set of standard attributes FAST FI' s keep in FAST format for attribute verification.), which the FAST system can provide if both C and M are FAST-enabled by their FI's

During the connection with C, something on C' s computer, alerts M' s web server that C is FAST-enabled. It may be something like a permanent cookie placed on C' s computer by CFI when the customer signed up for electronic banking. It may be something else. The key point here is that C does not have to download any FAST software to participate. Whatever it is, M's web server becomes aware that C is FAST enabled and can pull C' s ID, which includes CFI' s ID, off of C' s computer to create a unique ID for the C/M attribute verification transaction. This occurs when M presents a screen asking permission for M to verify C' s 21 or over attribute. When C clicks the "verify me" button a second screen pops up with a list of standard FAST attributes and C clicks the 21 or older attribute, which gives M approval to verify the attribute with C' s CFI. C has no software plug-in or special software to accomplish this. M has special software called an "agent" provided by its MFI to accomplish this.

Step 2a, 2b M Creates CMID/T And Sends It To C And MFI

Both C and M have FAST IDs, which include their respective FI' s IDs. This enables M to combine the two during the transaction with C by pulling C' s ID off of C' s computer and combining it with M' s ID to create a combined ID called CMID. The attribute request (T for transaction) is added to this to create a unique transaction ID called C MID/T. This contains a time to live (TTL), which limits its use to a certain time period or number of uses. Since each FI supplies its own TTL to the C or M ID the lowest TTL prevails if there is a difference. This information is reflected on the MO rectangle in the graphic. (Note: the TTL determines how long the CMID/T stays active. At the end of this period, it cannot be used for the transaction but it is still stored so that it can be retrieved if there is a dispute or other problems.)

Step 3a C Forwards CMID/T to CFI

This paper assumes the CMID/T has information on it that instructs C' s browser to establish a secure (SSL) authenticated (passwords or PINs) connection with CFI. How this is done is unclear at this time. The idea behind the FAST technology solution in Use Case One is that the entire attribute verification transaction takes place quickly while C remains online with M so that M can complete the purchase transaction when it receives the attribute verification. How does C now go out of the connection with M to establish a separate secure and authenticated connection with CFI so that CFI knows the request comes from C? Unanswered, this question raises the issue of control and authorization. If we instead have M forward it through MFI to CFI, or M directly to CFI, how does CFI know C was really authorizing it without C giving his/her security password, etc.? The technology workgroup people assure the writer that they have a solution for this problem. One possibility would involve a button that might pop up on C' s screen after the

CMID/T is created so C can open a second line to its CFI and give its security password or PIN to CFI. This would not be viewable by M.

Step 3b MFI Registers CMID With MO And Retrieves Attribute Answers From MO

When MFI receives the CMID/T it is logged and stored. The CMID is then sent to MO without the attribute request (In this case "age 21 or over."). Instead the CMID is sent to MO with XML electronic tags that will pull the attribute answers and send them to MFI when CFI supplies them to MO. MFI may charge M at this point for the services performed. The transaction is designed so M will not be able to determine the identity of CFI.

Step 4a, 4b CFI Registers CMID/T With MO And Supplies Attribute Answers; MFI Picks Up The Answer And Forwards It To M

After authenticating that the CMID/T came from and was authorized by C, CFI logs and stores it. Then, CFI writes the answers to the attribute request on the CMID/T in such a manner that the attribute requested is not listed, only the answer gets attached to the CMID (usually yes or no). XML electronic tags, which identify it as the attribute answer, are also attached and it is forwarded to MO. At MO, the two CMIDs are matched and the two sets of tags operate to pull the answers and forward them to MFI. MO logs and stores the CMID transactions so if there is a later claim or dispute, MO can act as an independent third party to establish what occurred. Because of the electronic nature of the information, it may be possible to deal with claims or disputes in an automated fashion. It is important to note that the actual attribute information is stored at the FI' s. The only information that moves to MO and out to MFI and M is the answers to the request. So, in the age 21 or over example, the only attribute information that moves to MO and out to MFI and M is "yes" or "no". Given the TTL even this is only readable for a limited time. So, FAST transactions have strong privacy and security aspects.

Step 5a Optional Notification Of C

Step 5b Optional Notification Of M

2.3 CLAIMS HANDLING AND DISPUTE RESOLUTION IN USE CASE ONE

Claims and disputes in FAST can roughly be divided into two kinds: those that can be largely handled by reference to the electronic databases held at the FI' s and MO; and those that cannot. If there is a question of what was requested and what answer was given, this can easily be established by the electronic records. In our CFI, MFI example, if there is a disagreement about an electronic record this can be settled by accessing the MO records. Claims and dispute resolution can be initiated by a screen a customer can access through its FI or software already loaded on the customer' s computer or web server.

Many claims and disputes will not be able to be resolved by reference to electronic records only. FI' s will make mistakes or be fooled when identifying customers or verifying their attributes. A false driver' s license could be used to establish a false identity or age, for example. The FAST developers must decide how the FAST rules will deal with mistakes in identity or attribute

verification. The issuing party FI will probably make most of these mistakes. It does the identification of the issuing party and vouches for the accuracy of the issuing party' s attributes. It examines the issuing party' s identification papers (driver' s license, passport, social security card etc.). It handles the issuing party' s financial accounts. It converts this attribute information into electronic format as required by FAST. It establishes a security procedure (password or PIN number) for authenticating that it is communicating with the issuing party.

If there is a mistake, the relying party is harmed and under FAST rules should have the right to make a claim to recover a limited amount for a loss it may have suffered as result of the issuing party FI' s mistake (I am assuming the mistake was there). It is clear that the relying party should make its claim through its FI. The relying party FI is its point of contact with FAST. The relying party has its FAST contractual provisions in its home banking (in the case of C) or merchant contract (in the case of M) with its FI and was FAST-enabled by its FI. However, the mistake was made by the issuing party's FI. The relying party has no relationship with the issuing party FI, and probably doesn' t know who it is since FAST may be designed to keep this fact secret for privacy reasons. Therefore it must depend on the relying party FI to forward the claim and collect damages from the issuing party FI. In essence, the relying party FI acts as the relying party' s representative in claims handling and dispute resolution.

An alternative procedure might be a purchased warranty approach similar to what Identrus and others have established using a similar four-corner model of issuing and relying parties and their FI' s. Here customers agree to a complete waiver of liability for a FI mistake in identification. However, a relying customer has the option of purchasing a warranty for a set amount from the issuing party FI. The warranty is purchased through its relying party FI. However, the relying party FI has no liability for the warranty. It only acts as a conduit to the issuing party FI. The rules are clear that only the issuing party FI is liable under the warranty and only for direct damages, not consequential or punitive damages. If there is a problem the relying party files its claim with the relying party FI that again only acts as a conduit to the issuing party FI. The rules could also provide for mediation and binding arbitration if the relying party is not satisfied with the result. (If this approach were followed the identity of the issuing party FI would probably have to be revealed to the relying party.)

Is this a viable approach for FAST? Probably not. There needs to be some evidence that customers in the transactions that FAST might target, would be interested in purchased warranties. If FAST is an add-on to a home banking contract, it might not be advisable from a marketing and customer relations' perspective. Also the warranty adds more complexity to the transactions. The effectiveness of liability limitation provisions is discussed in Section 3.4.1. A possible solution for FAST might limit FI liability to actual damages up to a set maximum amount. This could be combined with a warranty system somewhat similar to what covers the check world. The issuing party FI would warrant to the relying party FI that the identity and attribute information it forwarded is correct. The relying party FI would make the same warranty to the relying party. In essence, the FI' s each would warrant that the I/A information they forwarded is correct. (The legal question of whether banks can make such warranties needs to be researched.) This allows the relying party to file a claim and collect from the relying party FI. The relying party FI in turn has a right to file a claim and collect from the issuing party FI. A rough description of a process like this is described in Attachment 1.

FAST developers should also consider the need to establish a dispute resolution mechanism to resolve matters that cannot be resolved quickly. It might consist of an FI operated group that would mediate or arbitrate disputes.

The warranty approach:

- Puts the responsibility on the issuing party FI to identify its customer and his/her attributes correctly;
- Allows the relying party FI to tell its customer it warrants the I/A verification for a limited amount;
- Gives the relying party FI an unambiguous right to recover a limited amount from the issuing party FI; and
- Is a way to market FAST.

In summary, FAST developers could choose among several approaches:

1. Complete FAST FI disclaimers of liability similar to what credit bureaus do.

2. Complete disclaimer as above unless the relying party purchases a guarantee (warranty) for a set amount (similar to Identrus).

3. The warranty approach similar to that used in the check world as described above, with or without liability limitation provisions.

4. No warranty or contractual liability limitation provisions. Let the chips fall where they may.

2.4 THE DECENTRALIZED CENTRALIZED FAST TECHNOLOGY SOLUTION

The FAST technology solution described in this paper is the result of a series of adjustments that made a centralized version of FAST more decentralized. Originally, the centralized version envisioned a centralized switch and a centralized repository. The switch was to be run by a separate entity called FASTCO that moved the data back and forth between FI' s and customers. One version had FASTCO acting as a central repository for the attribute data. Legally, FASTCO would actually operate and be responsible for the switch and repository.

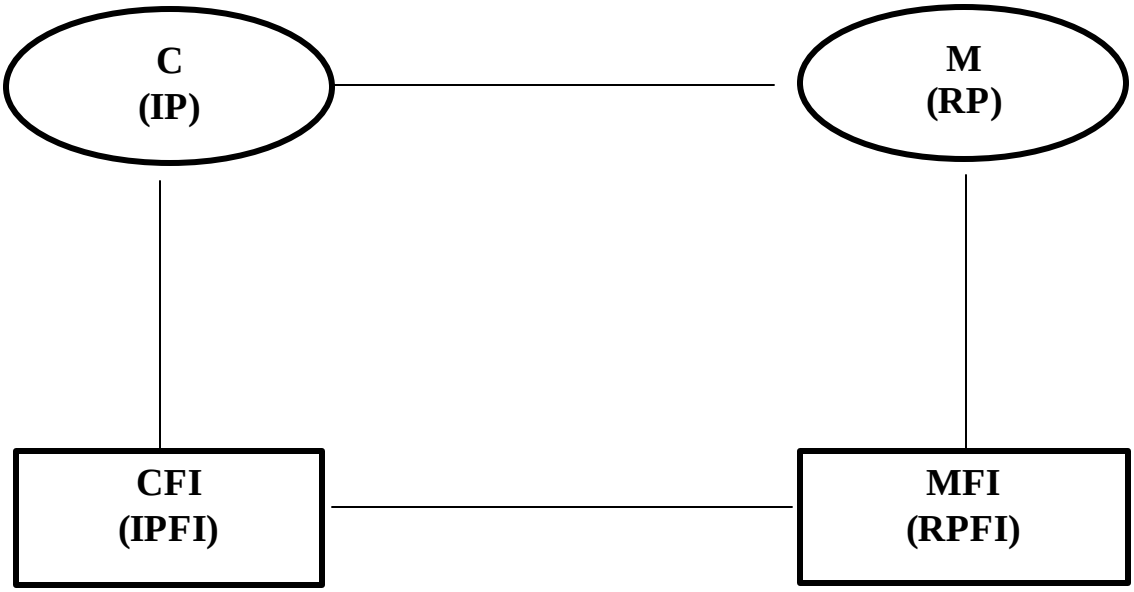
Under the current technology solution, this approach was decentralized so there is no FASTCO, no switch, and no repository. Instead, the MO sets common minimum standards, rules, contractual provisions etc. The FI' s or the application service provider acting on behalf of a group of FI' s, actually run the technology solution in a decentralized fashion from many points. FI customers only contact with the technology solution is through their FI. This and the FAST contracts and rules may insulate the MO entity from most liability for the operation of the technical solution. Likewise, FAST developers may want to consider FI/MO contractual provisions that effectively insulate a FAST FI not involved in a particular transaction, from liability for the negligence of another FAST FI participant.

3 LIABILITY ANALYSIS

This section looks at FAST liability risk in terms of issuing parties and relying parties as described in Section 2.2.2. For clarity and simplicity a four corner graphic with the following initials will be used:

- IP – issuing party
- IPFI – issuing party FI
- RP – relying party
- RPFI – relying party FI

The graphic depicted below is for a transaction in which M (RP) asks C (IP) to supply a FAST identity and age 21 or over attribute verification. MO and the transaction arrows are not shown on the graphic for simplicity.



3.1 FOUR CORNER WARRANTY MODEL

Earlier in this paper, I discussed the various ways FAST might structure the liability for an I/A verification forwarded to a relying party such as the merchant requesting an age 21 or over verification shown in the graphic above. I concluded that a warranty of the I/A by the issuing party FI (CFI) was one possible approach. It was responsible for checking the identity and attributes of its customer and should be required to stand behind and vouch for it. However, the issuing party FI has no contact with the relying party (the merchant) in the graphic. Instead, the merchant' s FAST contact is with its MFI (the relying party FI) in the graphic. Accordingly, I suggested that the FAST rules could provide that the issuing party FI (CFI) warrants the accuracy of the verification to the relying party FI (MFI) that in turn warrants its accuracy to the relying party (merchant).

Later, if there is an error in the verification, the relying party (merchant) files a claim with its relying party FI (MFI) which is solely liable to the relying party (merchant) under FAST rules. The relying party FI (MFI) then has the right to recover under the warranty from the issuing party FI (CFI) that made the mistake in identification. Under this liability structure, the relying party (merchant) has no right to recover from the issuing party FI (CFI). In fact, the relying party (the merchant) probably does not even know the identity of the issuing party FI (CFI). This is a clear, simple liability structure that places the liability on the customer' s FI. This approach could be combined with effective liability limitation contractual provisions. Otherwise FAST FI' s could be subject to open-ended liability for errors. FI' s could limit their liability for errors to a maximum figure that is reasonable given the fees charged for the verification warranty. By comparison, credit-reporting agencies exempt themselves from all liability for errors and are still widely used.

This is a contractual approach to limit the tort liability that may result from a FI' s mistake in issuing an I/A verification. An extreme example may highlight the issues that will be addressed in this section. Assume a FAST FI checks the identity and attributes of a customer either over the Internet or in-person and the customer signs the standard FI customer contract that includes standard FAST language. Later the FI (CFI on our graphic) issues an age 18 or over I/A verification at the request of its customer to the MFI of a gun merchant. Because of the technology of a FAST transaction, the CFI knows nothing about the merchant (the relying party in our graphic). It doesn' t know it' s name or that it is a gun merchant. That is the way the FAST technology is designed. The merchant sells the gun and the buyer, who is in fact 17, kills and injures several members of his high school class. It becomes a big news story. The merchant is prosecuted by the state and the merchant and the two FAST FI' s are sued for wrongful death and personal injuries. The merchant also brings the FI' s in as third party defendants in the gun sale. The merchant tells the newspapers it sold the gun only after verifying the age of the purchaser with its FI. Will the FAST FI contract with the merchant which limits it' s liability (to $2,000 for example) stand up in such a highly charged environment, especially if the case gets to the jury. If any of the parties can get around the contractual limitations on liability, the case will be handled under tort law. Consequently, this report examines both tort and contract law and focuses on liability limitation approaches.

3.2 ABA STUDY

The following is based on the liability analysis, attorney Thomas J. Smedinghoff used in the American Bankers Association, 1998 report entitled Certification Authority: Liability Analysis ("the ABA report").[2] While there are major differences between the FAST structure and a certification authority (CA) structure, there are also strong similarities. Both are at risk for mistakes in identity and attributes. The liability analysis in the ABA report is an excellent review of the issues that need to be considered in FAST. It examined five primary areas of potential liability. Four have relevance for FAST and will be discussed. The writer stresses again that he is not an expert in this area and that experts should be consulted.

[2] Thomas J Smedinghoff, Certification *Authority: Liability Analysis,* (1998) available at ABAecom web page under News and Information, Policy Advisory Committee, www.abaecom.com.

1. Tort liability for negligent misrepresentation;
2. Breach of contract or warranty;
3. Liability for the conduct of others; and
4. Intellectual property infringement.

3.3 TORT LIABILITY – NEGLIGENT MISREPRESENTATION

" A tort is a civil wrong, other than a breach of contract, for which the law will provide a remedy…" Its aim is to protect the rights and privileges of persons against wrongful acts by others.[3] The FAST tort risk is difficult to analyze. First, FAST has many novel elements. FI-held private personal information will be forwarded and warranted, at the customer' s request, to another FI that, in turn, will forward and warrant the information to a relying party. In Use Case One the relying party would be a wine merchant. The relying party, (the merchant) will pay a fee and then use the warranted information as one element in making the decision to go ahead with the transaction. In Use Case One this would be the sale of wine to a customer.

If there is an error in the attribute or identity, it will most likely occur because the FI' s customer deceived it. For example, an underage customer could use a false ID to set up a bank account enabling the customer to purchase items a minor is not allowed to purchase (guns, intoxicating liquor, pornography etc.). If this is the case, the relying party (merchant) may be harmed by the mistake and could lose its license or be fined. FAST contracts between the FI and the merchant would attempt to cover this risk.
The more difficult risk to analyze is the third-party risk. In the intoxicating liquor example, the minor receives the liquor because the merchant relied, in part, on erroneous age verification from a FAST FI. The minor becomes intoxicated and has an automobile accident with injuries. The injured parties sue the merchant and the FAST FI' s. The merchant also attempts to bring the FAST FI' s into the lawsuit as third party defendants, alleging it made the sale because of the erroneous verification. This raises questions. First, is this a realistic risk scenario for the merchant and the FAST FI' s? Second will the FI' s liability limitation clause be effective? Third, will relying parties such as merchants, be interested in joining FAST if this is a risk and the FAST contracts limit the ability of relying parties to recover from FAST FI' s or bring them in as third-party defendants? The remainder of this section is a general review of tort risk.

Negligence has four elements:

- A legal duty to a person or class of persons;
- A breach of that duty;
- The breach causes harm to the person; and
- The person suffers damages as a result for which compensation is a remedy.

Under tort law a FAST FI is in the information business and has a legal duty to a person who engages the FI to provide the information service. This section will begin by examining the standard of care required of a FAST FI when engaging in the information business.

[3] Id. 4.1

3.3.1 Reasonable Care

This is the care an ordinary person would exercise in the same or similar circumstances. For FAST, the standard is the care a reasonable person in the same line of business would exercise under similar circumstances.[4] Banks regularly check identity and attributes when customers open accounts. So, there is a custom or standard in the industry. FAST, however goes a step beyond this. A FAST FI forwards I/A information with a warranty to others online for a fee. This is a new service for which there is no custom. FAST FI' s may be held to the standard of care banks exercise in electronic transactions or some other standard. The most important factors in applying a standard of care are the magnitude and foreseeable of the harm, the utility of the conduct, the difficulty of guarding against the injury and the relationship of the parties.[5] In other words, the greater the risk of harm, the higher the degree of care necessary. The novel aspect in FAST is the forwarding of customer information to a relying party for a fee. The forwarding FI does not know the details of the transaction so it often has no understanding of the importance of the information.[6] In some versions of FAST the issuing FI (CFI) does not even know the identity of the relying party. So it may be difficult to say that it could foresee a particular risk. It could be argued that the warranty aspect of FAST makes the standard of care meaningless. The FI is liable no matter what standard of care is required. However, it would become relevant if non-FAST third parties sued, if FAST customers were able to get around the FAST contractual limitations or FAST decided to use a liability structure other than the warranty structure mentioned here.

3.3.2 Strict Liability

This is liability regardless of fault and is generally applied to product defects that result in physical harm.[7] A FAST FI answer to an attribute request is a service, not a product in the strict liability sense.

3.3.3 Statutorily-Defined Standard Of Care

The writer is unaware of any statutorily defined standard of care for the collection, storage and transmission of identity and attributes. The certificate authority statutes deal with these issues but FAST FI' s are not engaging in certificate authority transactions. State statutes should be checked to verify there are no statutorily defined standards of care.

3.3.4 Self-Defined Standard Of Care

Should a FAST transaction be judged by the duties and responsibilities it has set for itself in marketing and transacting business, or should it be judged by higher minimum standards established by law for policy reasons? While FAST rules and contracts should attempt to cover this risk, if they do not, industry custom will be important. The ABA report reviews savings bank cases in which simple, inexpensive means of customer identification needed to be

[4] Id. 4.2.1
[5] Id. 4.2.1
[6] Note however, that the MFI may know the merchant' s business focus, for example guns or liquor.
[7] Smedinghoff, supra 4.2.3

implemented to avoid liability.[8] Simple inexpensive means of crosschecking identity and attributes may become new minimum standards for a novel business like FAST.

3.3.5 To Whom Does A Fast FI Owe A Duty?

To understand its liability for information negligence, a FAST FI must identify to whom it owes a duty of care. If a FI is sued for negligent misrepresentation based on an erroneous I/A verification, it must first determine whether it owed a duty of care to that plaintiff. The analysis begins by first examining the duties owed to persons with whom the FI has a direct contract. Then it looks to others in the FAST family covered by the standard FAST contract and operating rules. Finally it examines the duties, if any, owed to non-FAST third parties who claim they relied on misinformation and were injured thereby. The ABA report has an excellent analysis of these issues in Section 4.3.

3.3.6 Do Fast Contractual Limitations Protect Against The Range Of Risk?

The ABA report states at Section 5.2.5.2 that courts …" generally enforce exculpatory clauses unless they violate a state' s public policy or something in the social relationship between the parties would dictate against it." Within the FAST family of FI' s, MO, issuing parties and relying parties most of the liability issues could be covered by contract and operating rules, provided they are drafted carefully and entered into correctly. This is especially important when dealing in the consumer arena. However, even the most carefully drafted liability limitation clause may not protect against the gross negligence of a FAST FI or a FI' s failure to disclose or highlight the liability limitation provisions in an electronic contract at the time the customer signs up. Also, liability may arise because a contract was not carefully drawn and did not protect against a risk. A judge may give an extreme interpretation of contract provisions to achieve a particular result, especially in the consumer arena. Or a FI' s marketing people may go too far in advertising FAST and as a consequence a court refuses to enforce a liability limitation. Finally, the legal uncertainty of a situation may result in a FI settlement of a claim that seemed to be clearly handled by a FAST contractual provision. For all of these reasons and more, FAST FI' s and MO cannot totally rely on contractual provisions that seem to protect them. In short, some understanding of the risk beyond the FAST contract and operating rules needs to be considered.

3.3.7 Liability To Third Parties

The relationship between the information provider and a non-FAST third party claiming it relied on the information to its detriment is important for determining liability. For example, an accountant may owe a far greater duty for its report to a client than to a remote party with whom the accountant has no contract. Likewise, a newspaper owes less of an obligation to its readers who pay a small price to purchase a newspaper than to a stockbroker who charges substantial transaction fees to clients. The ABA report examined a series of relationships to determine potential certificate authority liability to third parties for misinformation.[9] Liability for the reports of accountants, financial information providers, and credit reporting agencies were compared. In each of the examples, the information provider produced a paper or electronic

[8] Id. 4.2.5 (b)
[9] Id. 4.3.2 (a through e)

document, which could be read by third parties. Misinformation in the document was the basis of the third-party lawsuit risk.[10]

A FAST I/A verification transaction is fundamentally different. As presently envisioned, there is no electronic or paper document similar to an accountant's statement, digital certificate etc. that a third-party could read and rely on. Moreover, there is no document that could list the FI's disclaimer of liability to third parties. Instead, a FAST I/A verification transaction results in an answer to an I/A question. Often the answer is simply yes or no. The relying party will receive this and use it as one of several considerations in deciding to act or not act. It is not intended for distribution to third parties and to do so might bring the relying-party under Fair Credit Reporting Act coverage in some situations. If it were distributed, a yes or no would be meaningless to a third-party unless the relying party also supplied the third-party with the question it answered. The FAST contractual and operating rules could prohibit forwarding of FAST FI verifications to third-parties and require the relying party to indemnify the FAST FI's for any loss caused by the forwarding of a verification to a third-party in violation of a FAST rule or contractual provision. The rules could also make clear that a FAST FI only warrants the I/A verification for one transaction. Any reuse would be at the relying party's risk. It is possible that FAST may develop a new product that is intended to be transferred to third parties, but that would require a different legal analysis than this.

3.3.8 Summary of The Torts Section

FAST will probably be a private system that covers all FAST participants in a web of contracts and operating rules. These contracts and rules would attempt to govern tort and other risk contractually. It appears to this non-expert in tort law that third-parties would not have a good basis for a lawsuit directly against a FAST FI because the FAST system, if structured properly, would give them little or nothing that they could claim they relied on. There would be no electronic or paper document similar to an accountant's statement that would enable a third-party to claim reliance. A third party would have to come up with another way. That way might involve a lawsuit against a relying party. The relying party might then attempt to add its FAST FI as a third party defendant. The FAST contracts could attempt to prevent this or at least limit the FI's potential liability to the amount of the FAST liability limitation. This assumes the FAST FI/customer contracts are written and implemented properly. The writer is not an expert in negligence litigation so experts in the field should be consulted.

3.4 CONTRACT LIABILITY

A FAST FI's contractual and warranty obligations depend on what law applies to FI I/A verification transactions. Article 2 of the Uniform Commercial Code (UCC) governs transactions in goods. The common law applies to transactions in services and more particularly, to information transactions.[11] The Uniform Computer Information Transaction Act (UCITA) that is beginning to be adopted in some states, covers software licensing and other aspects of commercial transactions. It would appear that a FAST verification transaction that results in an

[10] Id. 4.3
[11] Id. 5.1

answer to an I/A question is a service, not goods. Thus, Article 2 of the UCC would not apply. However, the provision of FAST software by MO to FI' s, and by FI' s to customers may come within Article 2 or UCITA. This will not be explored in this paper.

The common law governing contracts for services is process oriented, that is, it focuses on how the contract is performed. When a company represents itself as capable of doing particular work, a warranty is implied that it will be performed properly. This standard varies with the service provider' s business. FI' s, as service providers check the identity and attributes of customers when they open accounts and transact other kinds of business. Most FI' s also transfer information and funds electronically. As a consequence, the law may hold FI' s to a high standard when checking a customer' s identity and attributes. It may also hold them to high security and reliability standards when engaging in electronic transactions. However a FAST transaction is novel, so the application of the law is not predictable. That is why an effective private contract system is important.

3.4.1 Liability Limitation

Effective contractual provisions limiting the liability of a FAST FI for inaccurate I/A verifications should be a major consideration for FAST developers. Generally courts enforce liability limitations (also called disclaimers, liability waivers or exculpatory clauses) unless they violate a state' s public policy or something in the parties' relationship argues against it.[12] The ABA report reviews the case law on liability limitation clauses in burglar alarm systems to supply guidance for the issue of whether liability limitations in certificate authority contracts will be effective. It concludes that most jurisdictions have upheld provisions limiting liability and damage amount, holding that they are neither against public policy nor unconscionable.[13] However a review of the recent case law reveals that the issue is far from clear. In one case, for example, the burglar alarm system contract provided that the most a customer could receive if the provider was negligent was six times the monthly charge for monitoring the system ($144.). In fact the actual loss to the insurance company subrogated into the shoes of the homeowner, was $382,000. In this case the court refused to uphold the liability limitation provisions.[14] This occurred three years after an appellate court in the same state had upheld a burglary alarm liability limitation clause against the same defendant. In the earlier case, the court stated, "Absent important public policy concerns, unconscionability or vague and ambiguous terms," [liability limitation provisions will be upheld, provided] "the party invoking the provision has not committed a willful or reckless breach."[15] I suggest that FAST developers read both these cases as well as the ABA report on the subject. The typical burglar alarm system contract provides that the service does not provide insurance coverage for the underlying property.[16] In the burglar alarm cases the nature of the contract and the cost of the service were some of the factors considered. The courts point out that burglar alarm system contracts do not provide insurance coverage for the underlying property. They are not insurance contracts. If they were, the cost of the service would be priced much higher to reflect the high dollar risk undertaken by the

[12] Id. 5.2.5.2 and 5.2.5.4.
[13] Id. 5.2.5.4.
[14] Braden v. Honeywell, Inc., 8 F. Supp. 2d 724, (S.D. Ohio 1998)
[15] Nahra v. Honeywell, Inc., 892 F. Supp. 962,969 (N.D. Ohio 1995)
[16] Smedinghoff, supra, 5.2.5.4.

company. Likewise FAST will probably be a low cost service with liability limited to a small maximum amount, not dissimilar to the contracts, alarm companies and certificate authorities make use of, as described in the ABA report. In the burglar alarm cases the courts said the homeowner could buy insurance if he or she wanted complete coverage. Similarly, FAST contracts should make clear that the FI' s are not providing insurance. FAST might even want to consider offering purchased insurance from a third-party insurance company to its participating customers, much as VeriSign does for its customers in the certificate authority arena. This would clarify that FAST FI' s do not provide insurance-like coverage but provide a means for customers to purchase such coverage.

It should be noted that FAST transactions are much different than burglar alarm service agreements. A burglar alarm system is a product and therefore is covered by a stricter body of law, which makes it harder to invoke liability limitations. The writer has reviewed the case law on stop payment orders, accountant and attorney' s statements, and financial related statements in this area and there are cases both supporting and rejecting the general rule.[17] However, nearly all of these cases differ substantially from FAST, in that a FAST transaction does not result in a tangible document that can be read by others. Also, the fact that a FAST transaction does not result in a tangible document means there is no place for a FAST FI to place liability limitation warnings to third parties as an accountant might do on a financial statement. Perhaps a reader of this document will come up with a better analogous situation, which can then be researched for precedents applicable to FAST transactions.

Finally the writer has a few suggestions. Liability limitation provisions will be strictly construed against the drafter, especially if the drafter is the beneficiary of the provisions. That means FAST FI' s must carefully draft exculpatory language. Standard FAST language would be useful but there may be differences between the different states where FAST FI' s enter into customer contracts. So state differences, the place of the contract, a choice of law clause etc. need to be considered. Exculpatory clauses that exempt a party from tort liability that was intentionally or recklessly caused are generally unenforceable on public policy grounds. How this plays out in the financial arena needs to be researched. There may be few cases in which a liability limitation was declared unenforceable for public policy reasons in the financial arena but FAST is in new territory. It is more likely the liability limitation provisions would be unenforceable because they were not highlighted to customers entering into contracts. If they are buried in the middle of a long contract, a court may invalidate the liability limitation provisions. If, in addition to the contract, there is a one-page summary which includes a clear description of the exculpatory language in large, more conspicuous print, that is likely to increase its enforceability. Even better would be an "I accept" requirement after the provisions. A final consideration: indemnification clauses in FI customer contracts are a particular device FAST might want to use. The FAST customer (relying party) would agree in its FAST contract, not to forward the FAST I/A verification to a third-party or reuse it in a subsequent transaction.

[17] See especially the cases compiled in ALR under the category "liability limitation" or Howard Hunter, Modern Law Of Contracts, published by Warren Gorham Lamont, at chapter 17 on remedies, 1998.

3.4.2 Third-Party Beneficiaries

As mentioned several times in this report, many of the cases brought against information providers involve plaintiffs claiming to be third-party beneficiaries who relied on an accountant's statement, lawyer's opinion, financial report or some other tangible manifestation created by the information provider. FAST, as presently envisioned, provides little or nothing that can be passed on to a non-FAST third-party. So a third-party would have a difficult time trying to prove that it actually relied on the FAST FI's I/A verification. Furthermore, FAST will be a private contractual system governed by contracts. Consequently, non-FAST third parties would have no contractual connection (otherwise called privity of contract) with FAST participants. In most FAST transactions it would be difficult for a non-FAST third- party to successfully argue that the FAST contract was drafted to give the third-party or the class of third parties to which the third-party belongs, rights against a FAST FI. In the liquor or gun example, the FAST merchant deals with the consumer who purchases the gun or liquor, not with the person injured by the consumer. It would be a real stretch to extend the FAST FI's obligations to a fourth-party such as the injured person. A more likely approach a court might take to get at the FAST FI, (the deep pocket) would be to invalidate the liability limitation clause governing the merchant. If this were done, the merchant that is sued by the injured party for the sale of liquor to the minor could bring the FAST FI in as a third-party defendant and the FAST FI would not be able to successfully interpose the liability limitation provisions to avoid liability.[18] This risk could be reduced by offering a purchased insurance option to FAST customers, as VeriSign does. Another approach would be to refuse to provide FAST I/A verifications to merchants dealing in risky transactions like gun or liquor sales. Again the writer is not an expert in this field.

3.5 LIABILITY OF A FAST FI OR MO FOR THE ACTS OF OTHERS

FAST participant FI's and MO face a risk that liability could be alleged based on the torts or crimes of others. That risk may come from the actions of its own employees, agents or contractors. Add to this the risk of an electronic hacker attack.

3.6 INTELLECTUAL PROPERTY AND PRIVACY LIABILITY

Intellectual property refers to legal rights in intangibles like inventions, processes, creations and trademarks. The activities of MO or a FAST FI could violate or infringe on these rights, resulting in lawsuits, damages and injunctions against further infringement.

3.6.1 Patents

Patents are issued on a country-by-country basis. In the U.S. a patent is obtained by filing with the Patent and Trademark Office (PTO). U.S. patents expire 20 years after a patent issues. Any new and useful process or machine is potentially patentable. However, mathematical formulae and mental processes that describe existing natural laws are not patentable. Something as complex as $e=mc^2$ would not be patentable.

[18] See Hunter for a thorough discussion of third-party beneficiaries at Chapter 20.

Software is patentable. For many years it was only patentable if part of a physical machine or process. Otherwise, it was treated like a mathematical formula. That limitation was overturned gradually. The most influential recent case is State Street Bank and Trust v. Signature Financial Services.[19]. Now the test for software is a "useful, concrete, and tangible result". If it meets this test it may be patentable provided it also meets the test of novelty and non-obviousness. Business processes are also patentable. Given the heavy reliance on software and business processes in the FAST technical solution, patent infringement should be a major concern. One of the non-bank companies participating in Phase One of the FAST project mentioned recently that it had a patent that may cover part of what FAST is developing. There are 40,000 software patents in the U.S. with a couple thousand more added each year. The PTO has a poor system for searching software and pending patents are not discoverable until issued. Consequently, discovering if there is an infringement problem is expensive and difficult.

Patent infringement involves direct use or the use of an equivalent process, which performs the same function as the patented software. Indirect infringement occurs when an entity provides a service to a customer, which the customer uses to infringe a patent. Remedies for patent infringement include money damages, attorney fees and injunctions. The software industry is particularly at risk in patent infringement cases because so much of the cost of software is in the development phase. If infringement is discovered during rollout, most of the costs of the product have already been sunk into development. The actual production of software by comparison is a small part of the total cost. This puts the patent holder into a powerful bargaining position.

3.6.2 Copyrights

Copyright protects original works in a tangible medium. The owner has the exclusive right to copy, distribute and publicly display the creation. The software, documentation, formats and content for the FAST product is subject to copyright. Online transmission of copyrighted material is a form of copying and raises infringement issues. Again, damages, attorney fees and injunctions are remedies. FAST can reduce its chances of a copyright dispute by creating its own software, acquiring copyrighted material or licensing it from a holder. FAST should include contractual indemnification provisions in its supplier and license contracts.

3.6.3 Trade Secrets

The Uniform Trade Secrets Act enacted at the state level needs to be considered. For example, FAST may become aware of the security practices of a covered entity as a customer or licensee of a security product. The Act prohibits disclosure of a trade secret acquired under circumstances, which give rise to a duty to maintain secrecy.[20] Damages and injunctions are remedies.

[19] 149 F. 3rd 1368 (Fed. Cir. 1998)
[20] *See e.g. Illinois Code,* 765 ILCS 1065/2(b).

3.6.4 Trademarks

Trademarks are the words and symbols used to distinguish the goods and services of one person from another. The owner of a trademark has the exclusive right to use the mark in a particular market for particular goods and services. FAST must be concerned about its own use of trademarks in offering its services. Trademarks are protected at both the federal and state level. Others may already have a trademark on the name FAST.

3.7 PRIVACY

See Section 4.2 for a discussion

3.8 CRIMINAL LIABILITY

A FAST FI could make an error in checking an I/A, which could result in criminal prosecution of a relying party. If so would the merchant and FI's be pulled into the criminal prosecution? Liquor and gun violations come to mind. Is this a realistic risk?

4 REGULATORY ENVIRONMENT AND OTHER LEGAL CONSIDERATIONS

4.1 CONSUMER LAWS AND REGULATIONS

4.1.1 Electronic Fund Transfer Act (EFTA) and Regulation E[21]

- Applies to any electronic fund transfer that authorizes a FI to debit or credit a C's account.[22]
- Electronic fund transfer means any transfer of funds that is initiated through an electronic terminal. [23]
- If a FAST transaction includes the debiting or crediting of a consumer asset account at a FI, Regulation E will apply. Thus, escrowing or placing "a hold" on a consumer's funds would appear to be equivalent to a debit of that account since it affects the consumer's access to those funds. This needs to be researched.
- An attribute statement that "the funds are there" would probably not be a debiting of the account. However, given the changing balance of a transaction account this attribute would probably be of little use to a merchant.
- A warranty by the FI of the transaction amount would not be viewed as a debit or credit of a consumer account, but a FI would need to be compensated adequately to take this risk. The question of whether an FI has the power to make such a warranty needs to be researched.

[21] 12 CFR 205.
[22] Id .205.3(a)
[23] Id. 205.3(b)

- Under the FAST technology solution, a consumer in Use Case One would contract to become FAST enabled with its FAST enabled FI. Most probably, the FAST provisions would be part of the FI' s home banking contract with the consumer. Note that the disclosures under Regulation E for the home banking product would need to be tailored to cover the FAST product.
- Regulation E would not apply to business-to-business transactions.

4.1.2 Regulation Z (Truth In Lending Act)

Regulation Z[24] is applicable to consumer credit transactions. During FAST discussions some participants mentioned the possibility of adding a credit component to a FAST transaction. This was not explored in Phase One. If a credit arrangement becomes part of a FAST transaction involving a consumer, Regulation Z would become applicable. In this case, the contractual provisions would most probably be part of the consumer' s home banking contract with the FI. Regulation Z is a consumer regulation and would not apply to business-to-business transactions.

4.1.3 Regulation CC (Expedited Funds Availability Act)

If a consumer' s account at a FI is debited or credited during a FAST transaction, a FAST FI will need to take into account the funds availability rules of Regulation CC[25].

4.1.4 Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA)[26] is a federal act governing individual consumer reports communicated by a consumer reporting agency. It governs not only reports about credit but also about personal characteristics, mode of living or character that serve as a factor in establishing a consumer' s eligibility for personal, family or household credit. It does not apply to commercial credit. It also governs reports made for employment purposes. The definition of a consumer report does not include any report containing information solely as to "transactions or experiences" between the consumer and the reporting entity. Consequently, reports by a FI about its own "transactions and experiences" with its customer would not be a consumer report within the meaning of FCRA.[27] It appears that information taken from a customer verbally or by means of documents like drivers' licenses, social security cards etc. would be an experience with the customer within the meaning of FCRA. The writer discussed this interpretation with another attorney familiar with FCRA. FAST developers should verify this interpretation with a top expert in the field.

In a FAST transaction, the issuing party FI issues "experiential" information, at the customer's request, to the relying party FI, which then forwards it to the relying party. Would the relying party FI be "communicating a consumer report" within the meaning of FCRA? Note that the relying party FI would not be able to effectively argue that it is communicating its experiential information, since the issuing party FI collected the data, not the relying party FI. To avoid

[24] 12 CFR 226.
[25] 12 CFR 229.
[26] 15 USC 1681.
[27] 15USC1681a (d)(2)(A)(i).

FCRA coverage it could argue instead that it is only acting as a switch in communicating the information to the relying party. In fact, the FAST technology solution may be designed so the relying party FI cannot read the actual consumer information transmitted. Even if it could, it might only be a yes or no. A comparable situation might be a credit card authorization transaction in which consumer information is transmitted, but the FI is only acting as a switch and is therefore not subject to FCRA coverage. This should be verified with FI' s active in the credit card field.

In summary:

1. A FAST FI issuing information gained from its own experiences with a FAST customer should not be deemed to have issued a consumer report within the meaning of the FCRA. Accordingly it would not become a credit-reporting agency as a result of these kinds of FAST transactions.

2. A relying party FI forwarding FAST consumer information obtained from an issuing party FI, should act as a switch as much as possible to avoid FCRA coverage. It would be best if the FI did not know the consumer data being transmitted.

3. Relying parties that obtain FAST consumer information and forward it to others would probably meet the definition of a consumer reporting agency in FCRA, unless they could argue that they were only acting as a switch

4. MO would have to be careful not to hold the actual consumer data.

5. This is a consumer regulation and would not apply to business-to-business transactions unless there was some forwarding of consumer information.

4.2 PRIVACY

In November 1999, Congress enacted the Gramm-Leach-Bliley Act (GLB act), which has privacy provisions that cover FI' s. Regulators have issued regulations for comment that implement the privacy provisions of the act. The regulations will be published on May 12, 2000 and will become effective on Nov. 13, 2000. These comments are based on a preliminary review of the act. The reader should consult the final regulations. Obviously FAST FI' s are covered by the act. It would appear that the act's expansive definition of FI also covers MO either because it is owned by FI' s, because it provides services to banking providers or because it holds the log of the FAST transactions, which may contain consumer information. An application service provider that the acts on behalf of a FAST FI could also be covered as a provider of services to FI' s. Query, do MO or an ASP (application service provider) do business with consumers within the meaning of the GLB act?

Any company that does business with consumers must have a privacy policy and disclose it to them. A consumer is defined as an individual who obtains financial products or services from a covered FI that are used primarily for personal, family or household services. The privacy provisions in the GLB act have three basic requirements:

1. They prohibit a FI from disclosing any nonpublic personal information about a consumer to any unaffiliated third party unless the FI has provided the consumer with a reasonable opportunity to opt out of the information sharing.

2. Prior to sharing nonpublic personal information regarding any consumer, the FI must also provide the consumer with a notice that describes the FI's privacy policies and procedures, including the institutions policies for sharing information with affiliates.

3. A FI must annually provide each consumer that has a continuing relationship with the institution an annual notice describing the institution's privacy policies and procedures. At the FAST customer level, the new regulations need to be carefully reviewed to determine if the privacy exception for customer-initiated transactions is applicable. FAST is a customer-initiated transaction. The new regulations also need to be consulted about restrictions on the reuse of customer nonpublic information by FAST relying party customers such as merchants. FAST developers may want to consider restricting the reuse of nonpublic customer information by FAST customers such as merchants. Reuse may bring FCRA coverage in some cases.

Beyond the GLB act the privacy landscape for FI' s has shifted rapidly over the past year. For example, 20 state attorneys general investigated the information sharing practices of some of the largest banking companies with credit card operations in a matter involving U.S. Bancorp. Here U.S. Bancorp was sued by the Minnesota State' s Attorney General for selling consumer credit report information, as well as, actual account numbers. The lawsuit claimed this violated the Fair Credit Reporting Act. Recently, Chase Manhattan Corporation entered into a privacy settlement with the New York State' s Attorney General for violating its own privacy policy by selling account information to outsiders. It was alleged that Chase violated the state' s deceptive practice statutes. The " American Banker newspaper" in commenting on the settlement stated that state government was working to tie up " loose ends in the federal law". The Financial Services Coordinating Council' s Privacy Project is attempting to convince states to give the GLB act opt-out provisions a chance before passing opt-in laws. The council includes major financial organizations like the ABA and SIA.

FAST developers should consider if the MO contract with FI' s should require FAST FI' s to enact standard FAST privacy provisions or should the contract rely on privacy polices already in effect at most FI' s. Beyond this FAST must consider how its technology will limit the amount of privacy information about customers made available during a FAST transaction. The current FAST technology solution would operate so only minimal information would be available to the other parties in a FAST transaction. MO will operate the central technology, will match FAST transactions, respond to requests and store electronic records. The technology will hide most of the FI customer privacy information.

4.3 RECORD-KEEPING, RETENTION REQUIREMENTS AND LOGS

Under the FAST technology solution, transaction records and logs will be kept at the MO level. Records and logs will also be kept by both FI' s to a transaction. Whether there are certain MO

minimum requirements on how and how long the FI' s must store the data needs to be determined. MO contracts with FI' s could spell out the minimum technology, records, record keeping and logs, which FAST FI' s must have. These contracts could also spell out what law governs MO/FI transactions. If MO will be the primary record center, there may be a reduced need to have MO rules governing how and how long FAST FI' s keep records. At the FI level record keeping etc. will be governed by the laws and regulations applicable to its operation. How these apply would depend on its legal structure, choice of law decision, domicile state, kinds of transactions and regulations. This is complex matter and needs to be thoroughly researched. For example, if MO holds only identity and attribute information for FI' s there may be one set of considerations. However, if it also holds payment or credit portions of transactions another set of issues may need to be considered.

4.4 AUDIT TRAIL

Closely related to record keeping log issues are audit trail considerations. Again this needs to be researched both at the MO level and the FAST FI level.

4.5 CONTRACTING

4.5.1 FI/Consumer

The FI/consumer FAST contractual provisions could be part of the FI' s home banking contract with the consumer. MO could require FAST FI' s to have certain minimum contract provisions on FAST subjects like claims and dispute resolution. How this is presented to the customer and by what means (online or otherwise) could be a FI proprietary consideration not a MO consideration.

4.5.2 FI/Merchant

Under the technology solution currently being considered, a merchant would need a FI supplied Web server software plug-in to engage in FAST transactions. If so, there would be a specific FAST contract between the FI and the merchant which would need to be consistent with MO minimum standards for both the technology and contractual provisions. Again, how these are presented and by what means will generally be a FI proprietary matter, not a MO matter.

4.5.3 Business-to-Business

These kinds of transactions are not explored here and would vary depending on transaction type, size and nature of the participants, whether browsers or web servers were involved, etc.

MANAGING THE FAST RISK

4.6 USE A SEPARATE LEGAL ENTITY

The uncertainty and scope of liability in FAST transactions and in the FAST web of relationships argues for a separate legal entity. It should be adequately capitalized by its owners to assure that it stands as a separate entity, not as a mere liability limitation front.

4.7 BINDING CONTRACTS FOR ALL FAST PARTIES

MO should enter into binding contracts with FAST FI' s and FAST FI' s should enter into binding contracts with its FAST customers. The ABA report by a well-known expert in on-line contracting, recommends written contracts on paper signed in ink. Perhaps the federal legislation on this subject now in Conference Committee will make electronic contracting more effective. For now, paper and ink is best for high-risk situations.The legislation has since passed and been signed by the President. It was not considered in this legal analysis.

4.8 LIABILITY STRUCTURE

FAST contracts should provide for a clear liability structure describing the duties and responsibilities of each party to a FAST transaction. If the warranty structure described here is adopted, the relying party' s sole recourse could be to its relying party FI, even though the mistake was made by the issuing party FI. If the relying party FI fails as an institution or unreasonably refuses to pay a rightful claim, FAST must have a fallback procedure. Another liability approach not reviewed here would be a common pooling of risk arrangement. It would be similar to self-insurance arrangements. The Federal Reserve Banks use this approach.

4.9 INSULATE MO AND OTHER FAST FI' S FROM LIABILITY FOR OTHER FAST FI' S MISTAKES

FAST developers should consider whether FI' s and MO should be insulated by contract from liability for the actions of another FAST FI or MO itself.

4.10 FAST TRANSACTIONS COULD BE GOVERNED BY EFFECTIVE LIABILITY LIMITATION PROVISIONS

This is a vital requirement given the possible open-ended liability, which could flow from an erroneous I/A verification. While the FAST structure and rules may help protect FI' s against direct lawsuits from third parties and also protect against being dragged in as a third party defendant, there is no certainty in litigation. Experts in the filed should be consulted. Both the terms of the liability limitation and the manner in which it is presented to customers need to be handled carefully.

4.11 FAST CONTRACTS COULD HAVE INDEMNITY PROVISIONS

This discourages FAST customers from forwarding I/A verification information to third-parities.

4.12 MO AND FAST FI' S COULD PUBLISH STRONG PRIVACY POLICIES

These could refer to FAST transactions and attributes. Whether FAST customers, a merchant for example, need to display a FAST privacy policy reference when displaying a standard FAST attribute screen needs to be considered.

4.13 CONTRACTS AND OPERATING RULES

FAST contractual or operating rules could deal with:

- The application, registration and enrollment process;
- MO, FI and customer responsibilities;
- The collection, verification, holding, transmission, logging and retention of FAST attributes and transaction data;
- Timely modification, deletion, addition and revocation of data;
- Auditing considerations;
- Suspension or termination of FAST parties;
- Intellectual property ownership and rights;
- Indemnification;
- The list of warranties FAST parties make;
- The clear disclaimer of all warranties express or implied not incorporated in the contract;
- Limits on liability both for direct and consequential damages and;
- Choice of law for interpreting contracts and rules.

4.14 FAIR CREDIT REPORTING ACT COVERAGE NEEDS TO BE RESEARCHED

An expert in the field needs to be consulted.

4.15 THIRD PARTY RISK NEEDS TO BE ASSESSED

Determine how FAST contracts and rules can be drafted to effectively protect FI' s against third party lawsuits and third party defendant unlimited liability for providing erroneous I/A information.

4.16 CONSIDER OFFERING PURCHASED LIABILITY INSURANCE PROTECTION TO SOME CATEGORIES OF CUSTOMERS

This is discussed in Sections 3.4.1 and 3.4.2

5 COMMENTS

This section lists legal/risk matters not reviewed in this paper but relevant to FAST.

1. Regulatory approval for FI' s and FI holding companies to participate in the FAST system, MO and I/A transactions has not been explored yet.

2. Do FAST FI' s have the authority to warrant or guarantee FAST I/A verifications?

3. If FAST will be involved in payments transactions, how would it interact with existing organization like VISA, MASTERCARD, NACHA, etc? Are rules changes necessary for FAST to interact with these organizations? What about new payment approaches like PayPal, X.com, etc.?

4. Many states restrict the shipment of intoxicating liquors from out-of-state. At least two state attorneys general have prosecuted. Shippers are voluntarily refusing to ship to certain states.

5. How would state gun, pornography and intoxicating liquor laws affect FAST?

6. Home banking contracts already have many of the disclosures and contractual terms useful in a FAST contract. How would FAST be implemented as an add-on to the home banking contract?

7. When FAST technology is used by a FAST merchant etc, does FAST need to place a notice to users that FAST FI' s do not monitor the merchant' s site. FAST FI contracts with customers could disclaim liability for monitoring the site. Virus waivers also need to be considered.

8. Venue – FAST might need language to bolster the venue choice. For example, the Wine.com website says the sale takes place in California and Wine.com only acts as the purchaser' s agent in choosing the delivery service. This might not be possible in FAST where transactions occur throughout the U. S. Is there some other approach?

9. Anti-Trust considerations have not been explored.

10. The risks connected with use of an application service provider have not been explored.

11. Choice of Law – FAST contracts might contain a statement that " all parties agree that all FAST contracts and rules are governed by the laws of X state." Apparently there needs to be some connection to the state chosen.

12. A merchant or other FAST participant that forwards information it received from a FAST FI to non-FAST third parties might find itself covered by FCRA. See Section 4.1.4.

13. Should there be two levels of FAST FI' s. The upper level signs up the lower level FI. This reduces the burden on MO. Does this change dispute resolution etc.? This has not been explored yet.

6 ATTACHMENTS

6.1 ATTACHMENT 1: CLAIMS HANDLING AND DISPUTE RESOLUTION EXAMPLE

1. M (relying party) requested and received an "age 21 or over" attribute validation from its MFI (relying party FI). M, sold intoxication liquors to C based on the attribute validation. Subsequently, the State liquor control commission fined M, $1,000 for selling intoxicating liquor to a minor.

2. M contracts its MFI and alleges a mistake in the attribute validation. MFI sends M a claim form online, by mail or takes the claim over the phone. Alternatively, MFI directs M to the FAST button that brings up a list of choices including a claim form. M completes form and forwards it to MFI along with M' s stored CMID/T information on the transaction if done online. MFI receives claim form and pulls up its CMID/T information of transaction if done online. The claim form with CMID/T information is forwarded to CFI (issuing party FI), which warranted the transaction under FAST rules.

3. CFI pulls up its logged record of the CMID/T information and researches the claim. CFI records may include a photocopy of the driver' s license of C and a second piece of identification. FAST rules may require proof of attribute records etc. that CFI must produce or pay the claim.

4a. CFI decides to pay the claim and forward funds to MFI. MFI forwards funds to M.

4b. CFI requests more information from M and forwards message to MFI which forwards message to M. M attempts to comply with request and resubmits claim to MFI that resubmits claim to CFI.

4c. CFI denies claim and forwards message to MFI which forwards it to M. Alternatively, MFI attempts to mediate with CFI to settle matter before submitting the denial to M. MFI does this to preserve its good customer relationship with M. Alternatively, MFI might decide to pay M' s claim out of its pocket to preserve its good customer relationship with M. Perhaps FAST rules should allow MFI to institute a dispute resolution process at this point before going back to M with the denial. Final alternative would have MFI informing M the claim has been denied and informing M of his rights to appeal and engage in a dispute resolution process.

5. M contacts MFI and requests appeal form, completes it and files appeal with MFI that forwards it to CFI that denies it again.

6. MFI receives appeal and forwards it to the FAST mediation/arbitration group along with relevant CMID/T information and original claim form.

7. Mediation/arbitration group reviews evidence, requests additional information and rules on the appeal. If ruling is against CFI, it must pay the costs of the mediation/arbitration as well as the amount of the claim.

8a. MFI and CFI are informed of result if M is successful and funds are sent from CFI to MFI (for claim) and mediation/arbitration group (for costs). MFI informs M of result and credits M' s account with funds.

8b. If appeal is denied, the group sends a notice to MFI which MFI can then forward to M. This is better than having MFI actually deny the appeal.

Electronic Alternative

If the claim or dispute can be resolved by simply comparing the three CMID/T versions stored at the two FI' s and the MO database, then an automated claim approach would be useful. The winner would be determined by what is stored on the MO database. This would speed up the procedure and get all of the relevant information before the two FI' s immediately. Unfortunately, many of the claims will not be amenable to this kind of solution, for example a false drivers license problem. If the warranty system discussed in this paper is adopted this would simplify electronic dispute resolution.

Occasional Paper Series

Why Don' t Consumers Use Electronic Banking Products?
Towards a Theory of Obstacles, Incentives, and Opportunities
Brian Mantel EPS-2000-1

Legal Analysis of a Banking Industry Online Identify and Attribute Authentication Service for Consumers and Merchants: The Financial Services Technology Consortium' s FAST Initiative.
William Gram EPS-2000-2

Related Publications on Payment Systems

Chakravorti, Sujit (2000). "Why Has Stored Value Not Caught On?" Federal Reserve Bank of Chicago *Emerging Issues Series*. May 2000 (S&R-2000-6).

Chakravorti, Sujit and Ted To (1999). "A Theory of Merchant Credit Card Acceptance." Federal Reserve Bank of Chicago Working Paper Series. November 1999 (WP-99-16).

Green, Edward J. and Ruilin Zhou (2000). "Dynamic Monetary Equilibrium in a Random-Matching Economy." Federal Reserve Bank of Chicago Working Paper Series. February 2000 (WP-00-1).

Mantel, Brian (2000). "Why Do Consumers Pay Bills Electronically? An Empirical Analysis." Federal Reserve Bank of Chicago *Economic Perspectives*. Fourth Quarter, 2000. (Forthcoming).

Velde, Francois and Warren Weber (1998). "A Model of Bimetallism." Federal Reserve Bank of Chicago Working Paper Series. September 1998 (WP-98-8).

Zhou, Ruilin (1999). "Understanding Intraday Credit in Large-value Payment Systems." Federal Reserve Bank of Chicago *Economic Perspectives*. Third Quarter, 2000.

Zhou, Ruilin (1999). "Does Commodity Money Eliminate the Indeterminacy of Equilibria?" Federal Reserve Bank of Chicago Working Paper Series. October 1999 (WP-99-15).