

**DRAFT**  
**Report of the**  
**Identity Management Legal Task Force**  
**American Bar Association**

**Solving the Legal Challenges of**  
**Online Identity Management**

**PART 3**  
**Structuring a Legal Framework**  
**for an Identity System**

The views expressed herein have not been approved by the Council of the Section of Business Law, the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the policy of the American Bar Association.

Please submit comments to Task Force Chair:  
Thomas J. Smedinghoff: [tsmedinghoff@edwardswildman.com](mailto:tsmedinghoff@edwardswildman.com)

**TABLE OF CONTENTS**

<b>EXECUTIVE SUMMARY .....</b>	<b>1</b>
<b>SCOPE AND STRUCTURE OF REPORT.....</b>	<b>1</b>
<b>STRUCTURING A LEGAL FRAMEWORK FOR AN IDENTITY SYSTEM.....</b>	<b>2</b>
<b>1. The Nature of a Legal Framework.....</b>	<b>2</b>
<b>2. Goals of an Identity System Legal Framework.....</b>	<b>4</b>
<b>3. Structural Considerations for Legal Frameworks.....</b>	<b>6</b>
3.1. Creation -- Who Writes the System Rules? .....	7
3.2. Interface -- How Can System Rules Interface with Laws and Regulations? .....	9
3.3. Binding -- How Are the System Rules Made Binding on all Participants?.....	9
3.4. Enforcement – How Is Compliance with the System Rules Enforced?.....	12
3.5. Interoperability -- How Are the System Rules Made Interoperable? .....	13
<b>4. Basic Structural Models for an Identity Legal Framework.....</b>	<b>13</b>
4.1. Independent Governing Entity Models – (Collaborative Models) .....	13
4.2. Single Participant Governing Models – (Centralized Models).....	15
4.3. Mutual Agreement Models – (Collaborative Models).....	15
4.4. Bi-Lateral Participant Models.....	15
4.5. Other Models ??.....	15
<b>5. Addressing Privacy Risk .....</b>	<b>15</b>
<b>6. Addressing Liability Risk.....</b>	<b>16</b>
6.1. Basic Approaches to Allocating Liability for Losses .....	17
6.2. Justifications for Shifting Losses.....	19
6.3. Addressing Liability via the System Rules.....	20
6.4. Strategies for Addressing Liability .....	21
<b>7. Addressing Enforceability Risk.....</b>	<b>21</b>

## **Executive Summary**

*[to be completed after rest of doc]*

## **Scope and Structure of Report**

This Report examines the legal issues associated with the development, implementation operation, and maintenance of online identity management systems. Its primary objectives are to:

- Provide a general understanding of the concept of identity management sufficient to identify and analyze the legal issues;
- Identify the legal issues raised by the development, implementation operation, and maintenance of online identity management systems, both in the U.S. and internationally;
- Analyze those legal issues so as to better understand their impact and to evaluate possible approaches for addressing them where required;
- Identify existing law applicable to online identity management, and any barriers created by such law;
- Evaluate possible approaches to developing the Legal Rules for an identity system;
- Clarify the interaction between the technical controls and legal obligations of the stakeholders in an identity management ecosystem; and
- [Other??]

This Report is set forth in three parts, as follows:

- Part 1: Identity Management Fundamentals and Terminology
- Part 2: Legal Regulation of, and Barriers to, Identity Management
- Part 3: Structuring the Legal Framework for an Identity System

## **STRUCTURING A LEGAL FRAMEWORK FOR AN IDENTITY SYSTEM**

The System Rules that govern an identity system (as set out in Part 1, Section 7), operate in the context of a Legal Framework. That Legal Framework is, to some extent, defined by the author(s) of the System Rules (i.e., it includes the Legal Rules they write), and to some extent beyond their control (i.e., it includes existing laws and regulations). But that Legal Framework, as a whole, is the glue that holds the System Rules together, facilitates enforcement of the requirements of the various components of the System Rules, and governs the overall operation of the identity system.

Thus, the key to addressing the legal issues for any identity system is to structure (to the extent possible) an appropriate Legal Framework. Structuring a Legal Framework requires addressing three sets of issues:

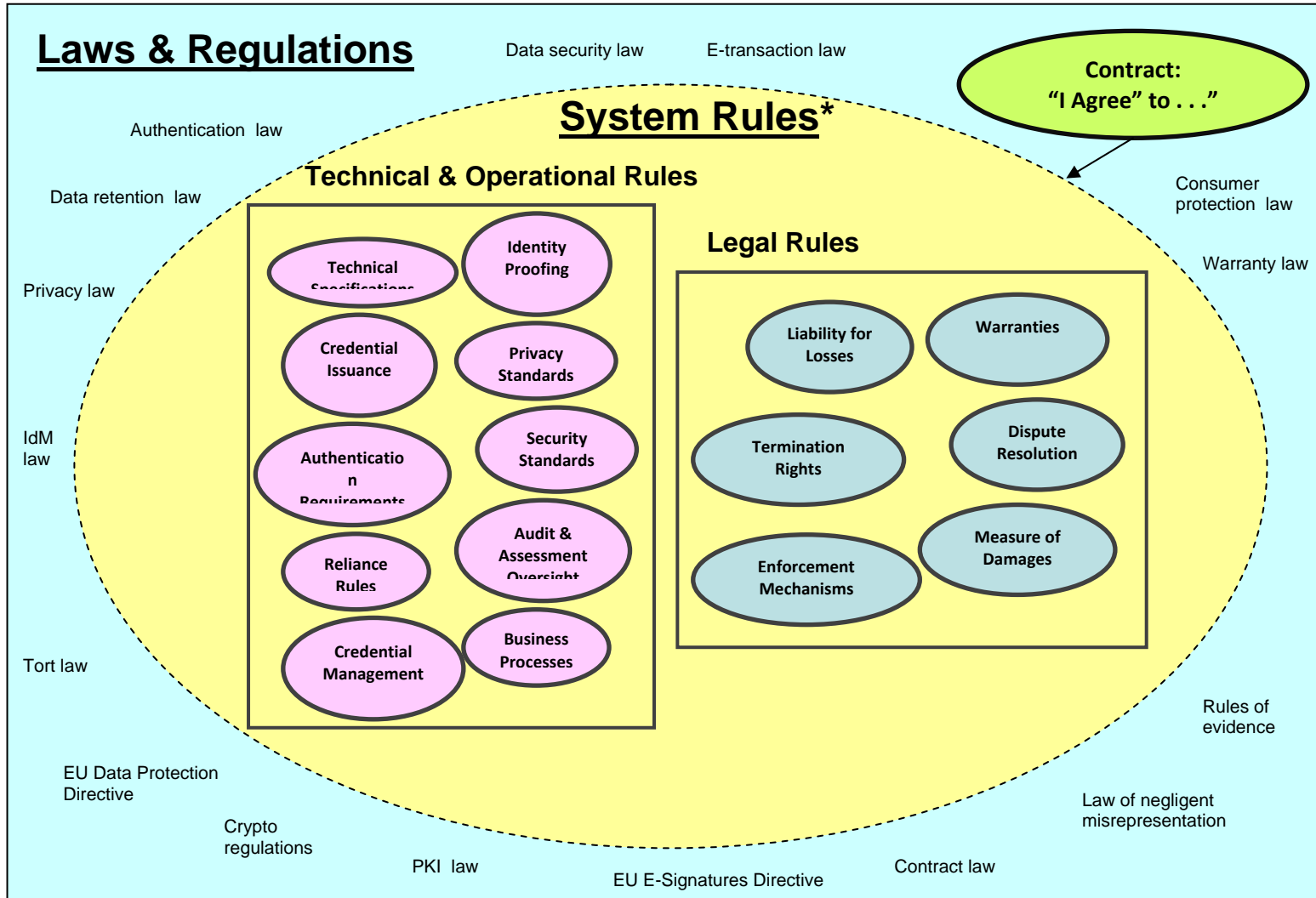
- Specifying the Legal Rules that will govern the conduct of the parties via the System Rules;
- Designing a contractual structure that will make the System Rules binding on all participants (to the extent applicable to each participant); and
- Ensuring that the System Rules and associated contractual structure coordinate and comply with existing laws and regulations across all applicable jurisdictions.

### **1. The Nature of a Legal Framework**

At its essence, the Legal Framework for any identity system is a combination of (1) the rules the parties themselves make up and agree upon (i.e., the System Rules, consisting of the Technical & Operational Rules and the Legal Rules), (2) the legal structure(s) they use (e.g., contracts) to make those System Rules binding on the participants, and (3) the existing laws and regulations (most of which were not written with identity management in mind) that address issues not covered by the System Rules, or which in some cases supersede the System Rules. The concept of a Legal Framework for an identity system is depicted in the diagram on the following page.

As this diagram illustrates, portions of the Legal Framework for any identity system (i.e., the System rules portion) are under the control of the developers of that identity system, and other portions are outside of their control. That is, they are free to make up the System Rules (so long, of course, as they don't violate any law and the participants agree to be bound by them), but at the same time, the private contracts that make these Rules binding on the participants are supplemented (and in some cases overruled) by existing laws and regulations. As such, the System Rules must interface with existing law – a challenge made all the more difficult for identity systems that cross jurisdictional boundaries.

## Legal Framework for an Identity System



\* a/k/a "Trust Framework"

The various credit card systems offer, by analogy, an example of what an identity system Legal Framework might look like. Operating internationally, each credit card system is governed by system rules (e.g., the Visa Operating Regulations) that specify both the technical and operational rules for the credit card system, and the legal rules governing the relationships between the various parties. Those system rules are made binding on the parties by virtue of a system of contracts, including the contracts between the credit card systems (e.g., Visa, MasterCard) and the card issuers (the banks), the contracts between the issuing banks and the merchants, and the contracts between the issuing banks and the cardholders. But those credit card system rules and that system of contracts are also governed by: (1) jurisdiction-specific general laws and regulations that were not written to address credit cards (e.g., the law of contracts, the law of negligence, etc.), and (2) jurisdiction-specific laws and regulations written specifically to regulate the credit card system (e.g., Regulation Z in the U.S.), both of which are also binding on the parties by force of law. This combination of private system rules, private contracts, and laws and regulations form the legal framework in which each credit card system operates.

Short of comprehensive and uniform legislation, it would appear that something similar is required for each identity system Legal Framework. And as illustrated by the credit card system analogy, it is clear that much of that identity system Legal Framework is under the control of those who develop each identity system. Structuring such an identity system Legal Framework begins with a consideration of its primary goals.

## **2. Goals of an Identity System Legal Framework**

While the ultimate goal of the System Rules for an identity system is to make the identity system work in a trustworthy manner [??], the goals of the Legal Framework are a bit different, primarily because they are focused on the legal aspects of the identity system.

The structure and content of the Legal Framework for an Identity system and its corresponding System Rules will vary across different identity systems. Likewise, the method and manner of the demarcation between public regulation (i.e., applicable existing laws and regulations) and private regulation (i.e., System Rules and contracts) may vary from case to case, but in all cases the goal should be ensuring that both the System Rules and the overall Legal Framework of which they are a part adhere to certain principles designed to make the identity system “work,” while removing legal barriers and promoting “legal interoperability.” Those principles are summarized as follows:

- **Legal Certainty and Predictability:** The identity system should be governed and regulated by a set of rules that clearly and unambiguously define the legal rights, obligations, duties, and responsibilities of each of the participant roles in a manner that creates a workable, reliable, and trustworthy identity system, and that provides appropriate legal certainty and predictability for all participants. This requires identifying applicable existing public laws and regulations, and then designing the private regulations (e.g., the System Rules and contracts) necessary to fill any gaps in existing law, to revise and/or clarify the impact of existing laws, and where necessary, to modify by agreement or opt out of inappropriate rules imposed by existing law. [*Optionally, it also requires making*

*clear to unsophisticated participants (e.g., consumers) the nature of their rights and obligations.]*

- **Validity and Compliance:** The System Rules for an identity system, and the contracts by which they are made binding, should be written and structured to be valid and in compliance with applicable law in all jurisdictions (including countries and their political subdivisions) with which the system or its participants have a jurisdictional nexus. This requires identifying applicable existing public laws and regulations in each relevant jurisdiction, and then designing the System Rules and contracts to ensure multi-jurisdiction compliance and/or to modify by agreement or opt out of rules imposed by existing laws and regulations where necessary and permissible.
- **Resolution of Cross-Jurisdictional Issues:** The System Rules that govern operation of an identity system should address differences in existing laws and regulations among applicable jurisdictions, so that they adopt an approach that is compliant with the law of all relevant jurisdictions. Such compliance can be achieved in a variety of ways, ranging from adopting highest common denominator rules that comply with the laws in all jurisdictions, to adopting different rules for different jurisdictions, to changing the rules in one or more jurisdictions by agreement of the parties.
- **Data Privacy:** Beyond compliance with applicable privacy laws, the process for development of System Rules should consider whether to impose additional requirements regarding the privacy of personal data. This Principle assumes a requirement to comply with applicable privacy laws and asks whether the System Rules need to go further in light of the nature of the particular identity system and its participants. In some cases, compliance with applicable law may be sufficient. In other cases, more stringent privacy requirements may be appropriate.
- **Data Security:** Beyond compliance with applicable data security laws, the process for development of System Rules should consider whether to impose additional requirements on the participants regarding the security of the identity processes and personal data to ensure trust in the process in a manner that is acceptable to the participants, is appropriate for the particular system, and engenders trust in its operation. This Principle recognizes that security is a relative concept that will vary from one identity system to another. It assumes a requirement to comply with applicable data security laws and asks whether the System Rules need to go further in light of the nature of the particular identity system and its participants. In some cases, compliance with applicable law may be sufficient. In other cases, more stringent data security requirements may be appropriate, especially as it relates to levels of assurance.
- **Risk Allocation and Liability Management:** The System Rules that govern operation of an identity system should clearly and fairly allocate risk and responsibility among the parties, address issues regarding the liability of the participants for their actions (or failure to act), and provide appropriate sharing or spreading of responsibility for “systemic” risks and liabilities, in a manner acceptable to the participants and compliant with applicable law. This Principle does not define “how” risk allocation and liability

should be addressed, just “that” it should be addressed in a manner acceptable to participants, appropriate for the particular system, and compliant with applicable law.

- Enforceability and Dispute Resolution: An identity system Legal Framework should provide reasonable means for all participants to avoid disputes, to resolve those disputes that cannot be avoided, to enforce their rights, and to obtain redress for compensable losses they suffer in accordance with appropriate dispute resolution and enforcement mechanisms. It should also provide a realistic enforcement mechanism and remedy in the event that a participant fails to act in the required manner (e.g., terminate its participation, or provide for the recovery of damages).
- Adaptability: An identity system Legal Framework should provide reasonable processes for the creation, adoption, and communication of changes in the legal rights, obligations, duties, and responsibilities of each of the participant roles. [*Consider whether this is too specific??*]

### 3. Structural Considerations for Legal Frameworks

Wholly apart from the content of any System Rules incorporated within a Legal Framework, the structure by which such rules are put in place, agreed to by the parties (and later amended), and enforced will be a critical factor for any identity system. Those structural issues are a function of the following three questions:

- Who writes the System Rules (e.g., does a central authority specify the rules and require other parties to agree to them, does one single participant determine the rules, do all of the parties negotiate the rules between themselves as needed, etc.)? Someone needs to develop the System Rules (i.e., the Technical & Operational Rules and the Legal Rules) for each identity system. A related query is who revises and updates the System Rules when necessary (e.g., does each modification require a renegotiation of the contract among the participants, does the central authority have the right to change the System Rules upon “notice”, etc.)?
- How Are the System Rules Made Binding on the Appropriate Participants – e.g., By law? By individual contract? Is there one master agreement that everyone signs? Does each participant sign a separate but identical agreement with a central authority? Are there multiple bilateral contracts? Part of this analysis also requires asking how non-parties obtain the benefit of the obligations imposed on participants by the Legal Rules.
- How is adherence to the System Rules enforced against any particular participant? – e.g., does each participant bring its own breach of contract claim? Is there centralized monitoring and enforcement by a federation operator? Does the government enforce?
- How Can the System Rules and Associated Legal Framework be Made Interoperable? – \_\_\_\_\_ [*Insert discussion*]

Several models for the structure of System Rules have been proposed<sup>1</sup> and are discussed in Section \_\_\_\_ below. In all cases, however, each model is a function of the foregoing factors, described in more detail as follows:

### **3.1. Creation -- Who Writes the System Rules?**

Perhaps the key threshold structural question for any System Rules model is who writes the component Technical & Operational Rules and Legal Rules. While such component parts of the System Rules may well include standards and frameworks written by other organizations (e.g., the ITU-T X.509 standard, the OASIS SAML standard, Kantara Identity Assurance Framework), someone must still select, modify and adapt such standards for inclusion in the System Rules for a particular identity system. Possible authors for the System Rules include the following:

Independent Governing Entity. It is common for an independent entity to be formed or designated for the specific purpose of developing (and updating and enforcing) the rules that form the System Rules. This is usually appropriate in the case of a large scale identity system that includes numerous identity providers and relying parties. Such an entity is sometimes referred to as a Trust Framework Provider or Federation Operator.

Such an independent governing entity is an organization that defines or adopts the System Rules for an identity system, and then certifies for participation those identity providers, relying parties, and other participants that are in compliance with the System Rules. This approach has been referred to as a *Collaborative Model* – i.e., a group of founders forms an entity that establishes the rules for the operation and governance of the identity system, and then also undertakes the day-to-day governance of the identity system.<sup>2</sup> [In many cases, the various stakeholders that form the identity system also participate in the development of the rules (along with the independent entity), similar to the mutual agreement/Consortium Model described below.]

Examples of entities formed for this purpose include SAFE-BioPharma, IdenTrust, TSCP, and the CA/Browser Forum. Outside of identity, familiar examples of this approach

---

<sup>1</sup> See, e.g., Liberty Alliance Project, Liberty Alliance Contractual Framework Outline for Circles of Trust (undated), available at [http://projectliberty.org/liberty/files/whitepapers/liberty\\_alliance\\_contractual\\_framework\\_outline\\_for\\_circles\\_of\\_trust/?f=liberty/files/whitepapers/liberty\\_alliance\\_contractual\\_framework\\_outline\\_for\\_circles\\_of\\_trust](http://projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust/?f=liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust); Transglobal Secure Collaboration Programme, TSCP's Proposed Models for Implementing the Common Operating Rules of an Identity Federation and the Associated Roles Required (October 13, 2008), available at <http://tscp.org/index.php/about-tscp/library>, and Jeff Nigriny and Randy V. Sabett, The Third Party Assurance Model: A Legal Framework for Federated Identity Management, Jurimetrics, Summer 2010 at 509 – 537; available at <http://38.99.228.149/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=54501005004PDFA03> (fee required).

<sup>2</sup> See The Liberty Alliance Project, “Liberty Alliance Contractual Framework Outline for Circles of Trust,” at pp. 4-8; available at [http://www.projectliberty.org/liberty/files/whitepapers/liberty\\_alliance\\_contractual\\_framework\\_outline\\_for\\_circles\\_of\\_trust](http://www.projectliberty.org/liberty/files/whitepapers/liberty_alliance_contractual_framework_outline_for_circles_of_trust)

include Visa, Inc. and MasterCard, Inc. for credit and debit transactions, and the National Automated Clearinghouse Association (NACHA) for electronic fund transfer transactions.

Single Participant Governing Entity. In other cases, a single existing organization may set up its own identity system for its own specific purposes and operate as a Federation Operator or Relying Party in that context. Such an organization (either an identity provider or a relying party) writes the rules for a system that it seeks to promote as a business (e.g., VeriSign, Facebook, or Google operating as identity providers) or implement for its own benefit (e.g., GSA, operating as an agent for various federal government relying parties). For example, the U.S. General Services Administration has done this for purposes of establishing an identity system to facilitate transactions with other federal agencies as relying parties. This approach has been referred to as a **Centralized Model** – i.e., a single founder sets the rules and governance for the identity system, and contracts individually with each other participant.<sup>3</sup>

Non-Governing Standards Organization. In some cases, an independent entity may be established to develop (and update from time-to-time) System Rules, but such entity will not itself actually govern the operation of an identity system. It may, however, certify participants (particularly identity providers) as compliant with its System Rules. An example is the Kantara Initiative, which has established an Identity Assurance Framework.<sup>4</sup> Kantara's Identity Assurance Assessment program accredits assessors and certifies identity providers against its Identity Assurance Framework for operational interoperability.<sup>5</sup>

Mutual Agreement Among All Participants. In other cases the System Rules are jointly written by the participants in an identity system, and memorialized in a mutual contract they all enter into. In such case there is no separate governing entity or standards entity. Examples include \_\_\_\_\_. [*Consider including some consortium examples here that also involve mutual drafting and agreement amongst the parties*] This approach has been referred to as a **Consortium Model** – i.e., a small number of founders form a consortium via a multi-party contract that sets the rules and governance for the identity system.<sup>6</sup>

While the System Rules for an identity system could be developed and negotiated among all of the participants in the system, this will likely occur only in very small identity systems or in bilateral arrangements (such as between an employer and a retirement account manager to facilitate employee single sign-on access). As identity systems scale, it is simply impractical for all of the actual and potential participants to negotiate the parameters of the Technical & Operational Rules and the Legal Rules that comprise the System Rules, just as it is impractical for all participants in credit card transactions to participate in the negotiation of the Visa Operating Regulations.

---

<sup>3</sup> Id.

<sup>4</sup> <http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework+v2.0>

<sup>5</sup> <http://kantarainitiative.org/confluence/download/attachments/41649275/Kantara+IAF-1300-Assurance+Assessment+Scheme.pdf>

<sup>6</sup> Id.

Bi-Lateral Agreement. In other cases, two parties enter into a bilateral contract that set forth the System Rules for their specific relationship. Examples include single sign-on arrangements between employers (acting as identity providers for their employees) and benefits providers (acting as relying parties to provide health or retirements benefits information using the userID and password issued to the employee by the company).

Legislation or Regulation. In other cases, the rules may be written by the legislature or a government regulatory agency and made applicable to all identity federations by law. This is done in some countries, such as Colombia, Egypt, Malaysia, \_\_\_\_\_.

No Rules. In other cases, no System Rules exist. The parties simply interact on an ad hoc basis, much as parties traditionally issue and use birth certificates, driver's licenses, and the like. *[Is this true of any online identity systems?? Are there examples??]*

### **3.2. Interface -- How Can System Rules Interface with Laws and Regulations?**

*[To be added]*

### **3.3. Binding -- How Are the System Rules Made Binding on all Participants?**

The System Rules for an identity system are, in essence, a set of privately-written rules made enforceable by a voluntary agreement of the parties. Thus, a key challenge is establishing a contractual structure whereby all relevant participants (identity providers, subjects, and relying parties) can contractually agree to be bound in a manner that makes the relevant portion of the rules enforceable against them, for the benefit of all other participants in the identity system.

In doing this, however, it is not necessary to make all of the System Rules binding on all of the participants. The rules that apply to Identity Providers regarding credential issuance and revocation, for example, would not apply to subjects or relying parties. Likewise, there might be some rules that can vary among similar participants. Just as some credit card terms vary by issuing bank or the credit-worthiness of the cardholder (e.g., annual fee, interest rate, grace period), the manner in which some rules are applied to some participants might also vary (e.g., price of credentials or credential verification, etc.).

The goal is to ensure that the System Rules relevant to each participant are binding on such participant. While this can be accomplished by an arrangement whereby each participant enters into a bilateral contract with each other participant in the identity system, this becomes increasingly cumbersome and unmanageable as the size of the identity system expands.<sup>2</sup> Various structural approaches to obtaining binding commitments of all parties that run to all other parties likely to be affected have been proposed. They may be summarized as follows:

---

<sup>2</sup> See, e.g., Nigriny and Sabett, *The Third-Party Assurance Model: A Legal Framework for Federated Identity Management*, 50 *Jurimetrics* 509 (Summer 2010) at 512 (noting the potentially large number of required bilateral contracts as the number of participants expands).

Contract Approach. Typically, System Rules becomes binding on a party when it enters into a contract directly agreeing to the rules or enters into a contract incorporating the rules by reference. But there are many different ways to structure such a contract. For example:

- Where the rules are written by an independent governing entity (e.g., SAFE-BioPharma, IdenTrust, or Visa), a participant might either (1) enter into a bilateral contract directly with that governing entity whereby the participant agrees to be bound by the rules as they currently exist and as amended in the future, or (2) enter into a bilateral contract with another participant who has contracted with the governing entity, the terms of which are wholly or partially dictated by the governing entity, and which incorporate rules as they currently exist and as amended in the future;
- Where the rules are written by a non-governing standards entity (e.g., Kantara or OIX), a participant might enter into an agreement with one or more other participants incorporating those rule by reference (where the non-governing standards entity is not otherwise involved);
- Where the rules are written by one key participant (e.g., Facebook, Google, VeriSign, or GSA), every other participant typically enters into a contract directly with that one key participant;
- Where a group of participants mutually agree on rules among themselves, all of the participants might simply enter into a multi-party contract with all of the other participants whereby they all agree to the rules; and
- In the case of government agencies writing rules for an identity system it uses to fulfill a government purpose, the rules it writes may become binding by contract (as with GSA) or by regulation (as with \_\_\_\_).

Conduct Approach. In some cases, a party can become legally bound to the rules via conduct interpreted (or specifically designated) as indicating its agreement to be bound. The CA/Browser Forum essentially takes this approach with respect to Identity Providers by providing in its EV SSL Guidelines that by issuing a credential denominated by the issuing Identity Provider as an EV SSL certificate, the issuing Identity Provider agrees to be bound by those rules.

Certification Approach. The process of requesting and receiving certification of compliance can be structured to bind the participant to the legal rules. For example, an entity may become bound to a particular set of System Rules by applying for and obtaining certification from an independent standards-setting entity that it complies with such System Rules, and then by asserting such certification. This may result, for example, when an entity applies for and obtains certification from the Kantara Initiative that it complies with Kantara's Identity Assessment Framework, and then displays the Kantara certification to potential relying parties.

Legislation or Regulation. All of the foregoing is superseded, however, by any applicable legislation or regulation that imposes legal obligations on participants in an identity system.

Rules Not Binding on All Participants. [*Consider example of EV SSL identity system, where rules apply to CA's, but not to Relying Parties.*]

To the extent the System Rules are built on one or more contracts, the legal obligations set forth in the System Rules will apply only to those who have agreed to the contracts. This raises concerns in the following situations:

- In identity systems involving large numbers of individual **Subjects**, there may be a problem obtaining the agreement of all of the Subjects to the terms of a legally binding contract. It just may not be practical to do so, or it may not be realistic to assume that Subjects will understand those contracts or conduct themselves in certain ways that require a fairly sophisticated understanding of the relevant identity processes (e.g., protecting credentials, secret keys, etc.).
- Likewise, in identity systems involving potentially large numbers of **Relying Parties**, it may not be practical to bind all potential relying parties to a contract. This is particularly true where the goal is interoperable credentials that can be used with numerous relying parties across numerous identity systems.
- The activities of any identity system, or its impact, may spill outside of the contractual group to persons not obligated by the system contracts. This might include, for example, persons who are the victim of fraudulent credentials, or situations where legitimate Subjects try to use credentials with relying parties that are not part of the Identity system.
- To the extent that the activities of any identity system (e.g., credentials) will interact with another identity system, or otherwise affect persons outside of the system (e.g., victims), this also raises the problem of parties not all being part of the same contractually-based System Rules. [Cross-certification problem]

In the case of Subjects, the problem of addressing the rights and responsibilities of individual human Subjects is a two-fold challenge. The first is legally binding Subjects to the responsibilities that must be imposed on them in order to make the identity system work properly; responsibilities that, in the absence of existing law, may only exist by contract. The second is ensuring that they have the rights against other participants in the identity system to which they are entitled – rights that, in the absence of existing law, may likewise only exist by contract.

In either case, obtaining the binding commitment of human Subjects (especially consumers) to the terms of a contract may well be a difficult undertaking from a purely practical perspective. That is, the logistics of getting consumers to agree to legally binding agreements presents a challenge simply from a consumer experience perspective, much less from the perspective of understandability and/or enforceability.

Perhaps the most difficult challenge for contract-based System Rules is the non-participant. Such persons do not, of course, contractually agree to the System Rules. Yet they may have rights [and responsibilities?], particularly in the case where they are injured. The best example of this is the person whose identity is stolen and used to obtain a fraudulent credential. In such case, the victim of this crime may suffer losses as a result of the use of the fraudulent credential. Yet such person has not contractually agreed to the risk allocation provisions of the Legal Rules, and most likely can rely only on existing publicly-created law.

A related issue is determining how the benefits of the System Rules will be extended to all other persons for whom they are intended. Many of the possible approaches to making the system rules binding on a participant do not involve directly contracting with all other parties who would like to obtain the benefit of those obligations. For example, if an Identity Provider enters into a contract with an independent governing entity whereby it undertakes an obligation to conduct in-person identity proofing and represents that it will always examine two government-issued IDs, how do relying parties obtain the benefit of those commitments? And how do non-participants get benefits as well? Agreeing to legal rules is not the same as making participants legally obligated to each other. However, the various participants can be legally obligated to each other in a variety of ways, including:

- By entering into contracts with each other;
- Where the rules to which they agree specify that everyone agreeing to the rules is obligated to everyone else who agrees to the rules;
- Where the rules create a legal duty enforceable by others in tort.
- Where the contract or the rules make others affected by a participant's performance an express third party beneficiary.

#### **3.4. Enforcement – How Is Compliance with the System Rules Enforced?**

Agreeing to the legal rules, even in a legally significant way, is only the first step. Parties must also consider how those obligations may be enforced, and by whom. Basic options include:

- Initial review and assessment of a potential participant's capabilities and processes to ensure that it is able to, and does, comply with the rules (often performed by the independent governing entity or a designated assessor auditor to whom it delegates the task);
- By regular audit by an assessor/auditor to verify continuing compliance, with penalties for infractions, even if they do not yet cause any harm to anyone,
- By ad hoc investigation of complaints by the independent governing entity (or an auditor to whom it delegates the task), with ability to impose penalties and compensate injured parties for infractions that damage another party;
- By each individual participant, who enforces claims for breach of contract whenever it suffers an injury (typically after-the-fact claims only)
- Enforcement by technology can also be important – e.g., if you don't comply with the technical specs it won't work.

Also, as a prerequisite, it is often important to address performance capabilities before allowing someone to contractually agree. System Rules impose performance obligations on participants in an identity system. And in some cases, such as with respect to identity providers, those obligations can be significant. This raises the question as to whether such participants should be evaluated before they are allowed to participate, to ensure that they have the capability and the necessary technology, procedures, and processes in place to meet those obligations. This can be important for assuring other participants that they have the requisite capabilities and credentials to properly perform their obligations.

### **3.5. Interoperability -- How Are the System Rules Made Interoperable?**

[To be added]

## **4. Basic Structural Models for an Identity Legal Framework**

The basic structures for an identity Legal Framework are primarily a function of who makes the rules and how participants are bound to those rules. The other considerations noted above can be incorporated in almost any model based on those two factors.

### **4.1. Independent Governing Entity Models – (Collaborative Models)**

A common approach to a System Rules for large scale systems is the use of an independent governing entity to make the rules, with everyone contractually bound to those rules (to the extent they relate to such participant). Some of the existing closed identity systems adopt such an approach, including SAFE-BioPharma, IdenTrust, TSCP, and \_\_\_\_\_.

There are two basic versions of the independent governing entity model. Under the first, every participant in the identity system enters into a contract with the governing entity whereby the participant agrees to be bound by the System Rules promulgated by the governing entity. Examples of this approach include SAFE-BioPharma, \_\_\_\_\_.

Under the second approach, one category of participants (e.g., Identity Providers) enter into a contract with the governing entity agreeing to be bound by the System Rules, and then members of that category of participants enter in to separate contracts with relying parties. An example of this approach is the 3PA Model proposed by Certipath initially for use within the TSCP, which is described as follows: [*summarize and clarify quoted text*]

“A proposed federation model that incorporates both the existing bilateral agreements between Identity Providers and RPs and utilizes a FO is the basis for the 3PA model. Specifically, the 3PA model incorporates the best features of the hub and consortium models and adds the efficiencies brought to bear by existing bilateral agreements. From the consortium model, the 3PA model incorporates contractual obligations via a common set of rules. From the hub model, the 3PA model incorporates maintenance and enforcement of the rules through a neutral governing entity.

In particular, like a federation that follows the hub model, the 3PA model has a governing entity, the FO, that either establishes a contractual relationship or has an existing contractual relationship with each of the Identity Providers in the federation. Leveraging these existing contractual relationships, when they do exist, provides a certain level of efficiency. Like a federation that follows the consortium model, the 3PA model involves a set of rules and governance provisions as the COR. Through contracts, these rules and governance provisions apply to all entities within the consortium.

The 3PA model, however, differs in several ways from the existing systems described above. In particular, the 3PA model creates a *double-binding* obligation on the Identity Provider to comply with the COR, taking the advantages of quasi-multilateral contracts executed with a hub and implementing them through standard two-party agreements. In effect, the Identity Provider has one set of contractual obligations directly applicable to it via its contract with the FO. The Identity Provider has a second set of contractual obligations to each RP in the federation (as a third-party beneficiary) via the incorporation by reference of the COR. Note that for certain RPs, the Identity Provider already may have certain obligations because of a preexisting contractual relationship with that RP.”<sup>8</sup>

Each of the credit card systems is a variation on this model. The credit card System Rules are set and revised from time-to-time by an independent governing entity (e.g., Visa, MasterCard). Some primary participants agree to those system rules by entering into a contract directly with the independent governing entity, whereas other participants enter into a contract with a primary participant, the terms of which are largely dictated by the system rules. Some of the participants (e.g., issuing banks) are members of the independent governing entity and have a voice in the process. Compliance with the system rules is enforced by the independent governing entity. The rules apply globally, but are subject to local law re e.g., credit card regulations. Identity providers (e.g., issuing banks) and relying parties (e.g., merchants and acquiring banks) agree to the system rules by entering into contracts with the independent governing entity or with other participants incorporating terms dictated by the system rules. Subjects (cardholders) agree by conduct (rather than signature) to terms set and revised from time-to-time by issuing banks, which terms are also subject to the system rules.

Another example is the electronic funds transfer payment system known as the Automated Clearinghouse (ACH). [Rules set and revised from time-to-time by the master entity (e.g., NACHA). Some of the participants (e.g., originating and receiving banks) are members of the master entity and have voice in the process. Compliance with rules is enforced by \_\_\_\_\_. Rules apply within U.S. (and globally??), but are subject to local law re e.g., EFT regulations, etc. Identity providers (e.g., originating banks) and relying parties (e.g., receiving banks) enter into contracts with \_\_\_\_\_ agreeing to be bound by the rules of the Master entity for each transaction. Subjects (originators of payment orders) agree by conduct or by signature to terms

---

<sup>8</sup> Nigriny and Sabett, *The Third-Party Assurance Model: A Legal Framework for Federated Identity Management*, 50 *Jurimetrics* 509 (Summer 2010) at pp. 523-24.

set and revised from time-to-time by \_\_\_\_\_, which terms are also subject to master entity rules.]

**4.2. Single Participant Governing Models – (Centralized Models)**

*[Examine, explain, and contrast such structures, e.g., Facebook Connect model, GSA FICAM model, etc.]*

**4.3. Mutual Agreement Models – (Collaborative Models)**

*[What multi-participant example systems are out there? Is this a realistic model??]*

**4.4. Bi-Lateral Participant Models**

*[Discuss model such as where employers act as Identity Provider for employees accessing benefits websites (e.g., health, retirement, etc.) in an SSO arrangement. Each arrangement presumably a one-off bilateral contract between employer and a particular benefits provider]*

**4.5. Other Models ??**

*[What other models are out there? Possible examples include Maritime Model; Franchise Law Model; DMV Model; Letter of Credit Model; Securities Regulation Model].*

**5. Addressing Privacy Risk**

Subjects are often concerned about the use of their personal data by identity providers and relying parties. In many jurisdictions, applicable publicly-created law imposes restrictions on the collection, use, processing, storage, transfer, and destruction of such personal data by identity providers and relying parties. Other jurisdictions, most noticeably in the United States, impose few if any such restrictions, except in certain sectors (e.g., the financial, healthcare, and public sectors). Moreover, the country-specific restrictions and regulations that do exist are not necessarily consistent. Thus, any contract-based System Rules must attempt to reconcile the competing privacy interests and competing legal requirements in a manner that is fair and equitable to all parties and that complies with applicable privacy laws.

The inconsistency in approach among jurisdictions regarding privacy may be one of the biggest hurdles to be addressed in developing an identity system Legal Framework. Examples of approaches used in existing System Rules to address privacy include the following: \_\_\_\_\_

**Possible Approaches**

- User-centric approach
- Enterprise-centric approach

EU Omnibus approach  
U.S. Sector-Specific approach  
Opt-In vs. Opt-Out approach  
Notice and Choice approach  
Harm-Based approach  
[Other Privacy approaches]

## 6. Addressing Liability Risk

Any identity system will at some point likely experience problems that will result in losses or damages to one or more of the participants or non-participants. A key function of the System Rules is to allocate the risk and liability for such losses among the participants in a manner deemed fair and compliant with existing laws and regulations.

A clear understanding of who is responsible for such losses, and who bears the risk of any resulting liability, is critical to developing those System Rules.

For any person or entity considering participating in an identity system, the so-called liability risk can be viewed from three perspectives:

- Risk of Loss: This is the risk of incurring one's own losses. It asks when (and to what extent) might an identity system participant suffer losses or damages as a result of participating? (e.g., if a Relying Party engages in a transaction as a result of a bad identity credential, what losses might it incur? If a Subject is unable to establish his or her identity in order to conduct a transaction, what damages might he or she suffer? Etc.)
- Risk of Liability: This is the risk of being held responsible for the losses of others. It asks when (and to what extent) might an identity system participant be held legally responsible for losses or damages suffered by someone else as a result of participating?<sup>2</sup> (e.g., if an Identity Provider issues a bad credential, and a Relying Party suffers a loss as a result, can the Identity Provider be required to compensate the Relying Party for its losses? If a Relying Party relies on a bad credential, and a data Subject suffers a loss as a result of the identity theft, can the Relying Party be required to compensate the Subject for its losses? Etc.)
- Risk of Non-Compliance: This is the risk of liability for civil fines or injunctions or criminal penalties, etc. It asks when (and to what extent) might an Identity system participant be held legally liable for civil fines or other penalties imposed by government agencies or regulatory authorities with respect to conduct in an identity system? (e.g., If the identity system involves the exchange of personal information about data Subjects in a manner that violates applicable law, the participant involved might be subjects to government enforcement actions and fines. If a relying party relies on a low level credential, might it violate a law or regulation requiring strong authentication?).

---

<sup>2</sup> Relatedly, when can such person hold other participants liable for the damages it suffers?

Regulatory compliance risk affects participants in an identity system in two ways. The first applies to the System Rules itself. That is, do the System Rules comply with the regulatory requirements imposed on the identity system and on the participants engaged in identity activities under that system?

The second applies to a participant's use of the identity system, and whether such use satisfies regulatory compliance requirements imposed on the participant. For example, under FFIEC Guidelines, banks must use sufficiently strong authentication processes to verify the identity of individuals engaged in online banking. For such a regulated bank, the regulatory compliance risk includes whether relying on a particular identity system will satisfy that regulatory obligation.

Concerns regarding one or more of these risks are commonly cited as key barriers to participating in an identity system. Thus, while the System Rules should be designed to minimize the occurrence of all losses, a key goal is to clearly define and allocate the risks of the losses that will inevitably occur, and to do so in a way that all participants perceive to be fair and acceptable.

For each participant, minimizing such risks, to the extent possible, is a critical concern. But all participants must recognize that where a loss occurs, liability is a zero-sum game. That is, if one participant is able to avoid responsibility for damages that flow from a malfunction of the system or failure of performance (such as through a contractual limitation of warranties or disclaimer of liability), the damages do not disappear. Instead, they must be borne by one or more of the other participants. Thus, from a legal perspective, the liability issue is one of allocating responsibility for losses, not eliminating them per se.<sup>10</sup>

### **6.1. Basic Approaches to Allocating Liability for Losses**

In the absence of any legal rule authorizing losses to be shifted from one party to another, the default rule is that any party suffering a loss must bear it.

In many cases, however, laws and regulations may shift losses from the party who initially suffered them to another party. Rules that shift responsibility for a loss suffered by one party are often imposed by statute, regulation, or common law. But in many cases rules governing responsibility for losses can also be agreed upon by the parties using a contract-based approach. In fact, in some cases, a contract may be used to modify the loss-shifting rule that would otherwise apply by statute, regulation, or common law. This is a key role of the System Rules.

Generally, there are three basic approaches typically used (in both laws and contracts) to shift responsibility for a loss suffered by one party to another. The most common approach is to shift the loss to the party that is in some way "at fault" or "responsible" for the loss. In some cases, however, losses are shifted to parties that are not responsible for causing the loss, but who,

---

<sup>10</sup> Of course, one of the goals of the System Rules is to design an identity system in a manner that minimizes the risk of losses by any of the parties.

for public policy reasons, it is felt should nonetheless bear the loss. These loss-shifting approaches may be summarized as follows:

- Fault-Based Approaches
  - Liability Based on Intentional Act or Omission: In some cases, the law provides that where the **intentional act or omission** of Party A<sup>11</sup> causes Party B to suffer a loss (e.g., battery, fraud, intentional breach of contract), Party A will be held liable for the loss suffered by party B (in some cases even where the intentional act was not malicious);
  - Liability Based on Negligent Act or Omission: In some cases, the law provides that where the **careless act or omission** of Party A<sup>12</sup> causes Party B to suffer a loss (e.g., negligence, negligent misrepresentation, negligent breach of contract), Party A will be held liable for the loss suffered by party B;
- Strict Liability Approaches
  - In some cases, the law provides that even though Party A has done nothing to cause Party B to suffer a loss, Party A will be held liable for the loss suffered by party B under a theory of **strict liability – i.e., liability without regard to fault**. This is a form of policy-based liability shifting often based entirely on which party is in the best position to either reduce losses or spread losses over a large group. This rule often arises **by operation of law**. For example, in the case of defective products that cause personal injury or property damage this rule is applied to hold a distributor of defectively manufactured goods liable even though it was not responsible for, and had no knowledge of, the defect. It also applies, for example, in the case of a stolen credit card, where the issuing bank is required to reimburse the cardholder for fraudulent charges. In some cases, this rule might arise on the basis of a **contractual agreement**. This might include, for example, a contract whereby a shipper agrees to reimburse the owner of goods destroyed by a natural disaster during shipment, or where a manufacturer warrants the performance of its product.

Fault-based approaches assign responsibility and liability for losses to the person whose conduct (or failure to act) was the proximate cause of the damage. To do so, however, requires establishing or adopting an appropriate standard against which to measure one's conduct – i.e., a standard against which to determine whether a person is “at fault” for failure to meet that standard. The law of negligence, where applicable, uses such an approach, measured against a “reasonable person” standard. Likewise, a court might find that a standard from a related law or regulation applies,<sup>13</sup> or the parties may contractually agree on a standard.

---

<sup>11</sup> Or a person for whom Party A is legally responsible (e.g., an employee, agent, subcontractor).

<sup>12</sup> Or a person for whom Party A is legally responsible (e.g., an employee, agent, subcontractor).

<sup>13</sup> See, e.g., *Guin v. Brazos Higher Education Service*, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006), adopting GLB standard.

Under a strict liability approach, one or more parties are held responsible for the losses of another, or are absolved from liability with respect to certain issues, regardless of their conduct or fault, typically for policy-based reasons. Examples where parties are absolved from liability regardless of their fault include the credit card model, where by regulation (in the U.S.) cardholders have no liability for losses resulting from their own negligence (or such liability is limited to \$50), and the driver's license issuance process, where by statute state government agencies issuing licenses have no liability for including incorrect data on the license. Conversely, under some models, policy considerations hold one or more parties responsible for any resulting harms and losses regardless of their conduct. Products liability law is a good example of this public policy approach. It holds the manufacturer and everyone in the chain of distribution liable for personal injury or property damage resulting from a defect in the product sold, regardless of their fault.

A warranty based approach is one type of strict liability approach. This approach considers what warranties each participant makes or is deemed to have made, and whether a loss suffered by any other participant results from a breach of any such warranty. Such an analysis assigns responsibility and liability for losses on the basis of whether a warranty was breached; whether the breaching party was at fault is not relevant. Thus, for example, if an Identity Provider is deemed to warrant the accuracy of an identity assertion, losses resulting from an incorrect identity assertion will be the responsibility of the Identity Provider even if it was not at fault in making the assertion – i.e., even if the Identity Provider followed all of the requisite standards and rules for identifying the Subject, but the result was nonetheless incorrect.

## **6.2. Justifications for Shifting Losses**

There are many different approaches and/or justifications for shifting losses from the party who initially suffered them to another party. For example, a party may be held liable for the losses of another when such party:

- Is the proximate cause of (or contributed to) the loss;
- Is legally responsible for the conduct of the party that is the proximate cause of (or contributed to) the loss (e.g., the loss was caused by an employee, agent or subcontractor under its control);
- Designed the system, process or product, or otherwise made the choices that ultimately led to the loss;
- Benefitted financially (or otherwise) from the system, process, or product that led to the loss
- Is in the best position to bear the loss
  - (e.g., a party that has a deep pocket)
  - (e.g., A party that is capable of pooling risks and distributing losses that occur over large groups (such as insurance companies or mass vendors who can average costs over large numbers of customers) are in a better position to bear risks than those who are not capable of pooling/averaging losses over large groups);
- Is in the best position to take measures or institute controls that could avoid, prevent or mitigate the loss;
- Has “ownership” or “control” over the subject of the loss (maritime model)

- Has a legal or moral obligation to protect the injured party; [??]
- Has contractually agreed to bear the loss;
- [other??]

Liability regimes can [also] be analyzed in terms of whether they **provide incentives** to the parties to minimize losses to the extent feasible. As a general rule<sup>14</sup>:

- Parties engaged in developing and managing the architecture of a system are in a better position to minimize losses than parties merely working within the architecture; and
- Parties capable of engaging in research and development of new risk management solutions are in a better position to minimize losses than end users or consumers whose only choice is to accept or reject a finished product.

### **6.3. Addressing Liability via the System Rules**

As a first priority, System Rules should be designed to do everything reasonably possible to reduce the risk and the magnitude of potential losses. But given that some losses will occur, the System Rules should also address the allocation of liability for such potential losses among the participants.

In doing so, it is important to recognize that liability is a zero-sum game. That is, protecting one participant from, or limiting its exposure to, liability for losses of certain types does not eliminate the losses themselves. It just shifts those losses to another party within the system.

Thus, addressing liability for losses in an identity system requires developing an approach that will be considered fair and equitable by all participants, accommodates the economic realities of the situation,<sup>15</sup> and complies with requirements of existing law. At the same time, the approach to liability of an identity system must also recognize that each participant may fill different roles at different times – i.e., that those roles may shift.

In most cases, the parties can use the System Rules as the vehicle to construct a liability scheme tailored to the needs of the identity system. That is, the participants can agree on their own rules regarding liability.<sup>16</sup> The most basic approach is where the parties simply negotiate and agree among themselves on an allocation of liability that is appropriate for the particular transaction. Such an approach works well in arms length bargaining among relatively sophisticated parties with similar bargaining power. It often raises questions of fairness, however, in the case of consumers or other unsophisticated parties with little or no bargaining power.

---

<sup>14</sup> Ronald Coase, *The Problem of Social Cost* (1963); Guido Calabrese, *The Cost of Accidents* (1973).

<sup>15</sup> In the U.S., for example, Uniform Commercial Code Article 4A recognizes that banks which charge mere pennies for high value electronic funds transfers cannot price those transactions in a way to address the potentially significant risk. So it allows the banks to avoid liability for certain risks if they adopt certain security measures.

<sup>16</sup> This may not be true in the case of consumers or government participants.

In the context of System Rules, allocation of responsibilities for losses can take a variety of forms. These include specifying when one participant will be responsible for the losses of another, imposing caps on the liability of one participant for the losses of another, and imposing restrictions on the ability of one party from taking action to restrict or limit their liability, such as by contract disclaimer, notice, or otherwise. The Uniform Commercial Code, for example, allows parties to limit their liability within certain parameters, but prohibits other limitations such as those that apply to personal injury. Likewise, the legal rules governing the issuance of EV SSL Certificates allows identity providers to limit their liability, but puts a floor on how much they can do so. A related approach involves the use of liability caps – i.e., that a party’s liability cannot exceed a certain amount.

Most likely, a Legal Framework for an identity system will need to adopt a combination of some or all of the foregoing approaches. And of course, it must also take into account existing statutory and regulatory risk allocation and liability rules that are the law in the relevant jurisdiction. For example, existing privacy and data protection laws may impose penalties on anyone misusing personal data regardless of any privately-agreed-upon rules to the contrary.

*[Discussion to be added]*

#### **6.4. Strategies for Addressing Liability**

*[To be added]*

### **7. Addressing Enforceability Risk**

*[To be added]*