Uniform Fiduciary Access to Digital Assets Act (UFADAA)

REPORT OF
LAW OF COMMERCE IN CYBERSPACE COMMITTEE
BUSINESS LAW SECTION
WASHINGTON STATE BAR ASSOCIATION

January, 2015

This report is submitted for approval by the Executive Committee of the Business Law Section of the Washington State Bar Association. Any approval will represent the view of the Business Law Section. The report has not been reviewed by the Legislative Committee of the Washington State Bar Association or by the Board of Governors, and therefore does not represent an official position of the Washington State Bar Association.

TABLE OF CONTENTS

A. Recommendations

The Law of Commerce in Cyberspace Committee ("Committee") is a committee of the Business Law Section of the Washington State Bar Association (the "Section"). The Committee recommends to the Executive Committee of the Section:

1. That the Executive Committee recommend against enactment of the Uniform Fiduciary Access to Digital Assets Act ("UFADAA") at this time. Although well-intended, UFADAA has the potential to create unintended surprise, harm or confusion and concerns material topics that cannot be resolved by state law.

2. The UFADAA should be amended before enactment by states. Non-uniform enactments will increase the above surprise, harm and confusion, so the UFADAA should not be adopted until amendment by the ULC.

B. What is UFADAA?

The Uniform Fiduciary Access to Digital Assets Act[1] ("UFADAA" or "Act") was drafted by the Uniform Law Commission ("ULC"). The stated purpose of UFADAA is to vest specified fiduciaries with the authority to access, control, or copy "digital assets"[2]. Digital assets are defined in UFADAA as "any record that is electronic" but not including an underlying assert or liability unless the asset or liability is itself a record that is electronic. "Digital assets" would include information stored on a computer device or on the Internet, including information stored in email, social media and photo-sharing accounts; according to the Act, they also can include information stored on tangible property[3] (e.g., Internet of Things). UFADAA grants access to digital assets to four specific categories of **fiduciaries** (defined as (a) personal representatives of deceased persons, (b) guardians of incapacitated persons, (c) "agents" of living persons who acting under a power of attorney, and (d) trustees of trusts.

At its simplest level, the Act is intended to deal with a situation like this: an elderly parent and a young teacher die or become incapacitated, leaving their respective executors to deal with traditional assets such as a house; apartment lease; bank account; mail; personal and business letters and records in a shoe box or file cabinet; and music, photo or book collections. The example includes two age groups because the amount and range of assets and records will vary for each.

In our digital economy, the above assets will expand. The parent and teacher are each called an "**account holder**" in UFADAA, a term meaning the person with a "**terms of service agreement**" with a "**custodian**" that "carries, maintains, processes, receives, or stores a digital asset of an account holder" such as Facebook. The digital items might include an online bank or stock account, a Drop Box account containing financial records of the small business run by the father, social media accounts such as at Facebook, dating sites, medical chatrooms, or private or "interest group" sites with photos, emails and chats about topics the account holder did not want to mention or store at home. When the account holder dies or becomes incapacitated, his or her executor or guardian (each a fiduciary) may need or want to deal with each account but might not have a required password or a right of access under the terms of service agreement.

The ULC has explained why a state should adopt UFADAA[4] as follows. The UFADAA:

- gives account holders control by allowing account holders to specify whether their digital assets should be preserved, distributed to heirs, or destroyed.
- treats digital assets like all other assets
- provides rules for common types of fiduciaries
- protects custodians (email service providers, ISPs, social media providers, etc.) and copyright holders.
- provides efficient uniformity for all concerned.

The intent of UFADAA is to allow a designated fiduciary to "step into the shoes" of the account holder[5]. The drafters do not intend that the designated fiduciary will have rights which are greater than the original

---

[1] Copy of final version with comments is available from http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/2014_UFADAA_Final.pdf.

[2] Prefatory Note to UFADAA.

[3] See Section 8(d).

[4] Uniform Law Commission "Why Your State Should Adopt the Uniform Fiduciary Access to Digital Assets Act"

account holder (and, indeed, under federal intellectual property laws some of those rights might not allow the fiduciary exactly to fill an account holder's shoes -- see No. 8 of this report). Such rights are typically established between the original account holder and the custodian by means of a terms of service agreement **("TOS**").

Although the Act understands its limitations, there is significant risk that fiduciaries, members of the probate bar and account holders not materially familiar with overriding federal laws (such as intellectual property laws and the ECPA discussed below) might incorrectly assume that UFADAA does more than it actually does and place false reliance on it. To illustrate, this article was written after Delaware purportedly adopted a "uniform" version of UFADAA:

Delaware Passes Law Which Makes eBooks and Other Digital Content Inheritable

19 August, 2014 Delaware, Law content, delaware, digital, ebooks, inheritable, law, passes Nate Hoffelder

Tweet 188 Pin it 40

Do you know that clause in the TOS for the Kindle Store and many other digital content stores which says that the content is licensed to you and is nontransferable?

The state of Delaware just negated that clause (in part).

Last week Governor Jack Markell signed House Bill (HB) 345, "Fiduciary Access to Digital Assets and Digital Accounts Act", giving heirs and the executors to estates the same rights over digital content which they would have over physical property.

In a case of life imitating art, the new law basically accomplishes what the Daily Mail fictitiously reported in 2012 that Bruce Willis wanted to accomplish; ebooks and other digital content can now be inherited.

[6]

The article completely misconstrues the Act, i.e., executors can merely see information about the digital assets or, in some cases, the asset itself, such as to determine what they are. However, when it comes time to obtain a copy or distribute them to an heir, the assets remain subject to contractual restrictions and federal copyright law, i.e., UFADAA does not make digital assets inheritable and could not, even if it wanted to. The fact that the article was written and published, however, illustrates the misunderstanding created by the Act and the material potential for debates among custodians and fiduciaries and the consequent cost concerns noted below.

---

[5] See – Memorandum from Kent to Walsh / Cahn dated March 10, 2014, page 1, http://www.uniformlawcommission.com/Committee.aspx?title=Fiduciary Access to Digital Assets

[6] (see The Digital Reader, article by Ars Technica, available at http://the-digital-reader.com/2014/08/19/delaware-passes-law-makes-ebooks-digital-content-inheritable/?et_mid=687718&rid=246705163)

C. What substantive concerns does UFADAA create?

1. ECPA. Portions of the UFADAA raise issues under the federal Electronic Communication Privacy Act ("ECPA").[7] The ECPA protects the contents of electronic communications from disclosure unless either the sender or receiver of such communication authorize such disclosure or unless other exceptions or conditions apply. The ECPA tends not to protect what UFADAA calls "catalogue of electronic communications" data such as the date, time and electronic address of a communication (e.g., who called whom and date and time) which is viewed under federal law as more akin to non-private "traffic" data (this data is not necessarily so viewed in all countries or under all state laws or by all individuals, e.g., note the Edward Snowden/ National Security Administration debate over collection of such "catalogue" data). The UFADAA seeks to avoid direct conflict with the ECPA by limiting the fiduciary's right to access certain digital information (i.e., content protected by ECPA) while preserving the fiduciary's right to access catalogue data.

A concern is whether UFADAA is misleading. For example (and subject to a rigorous opt-out exception), Section 4 states that the personal representative of the decedent has the "*right* to access," unless otherwise *ordered by the court* or provided in the will of a decedent, the catalogue data as well as the *content* of an electronic communication that the custodian is **permitted** to disclose under the ECPA.

Custodians will not necessarily know when they are "permitted" to disclose content. Section 10 of UFADAA contains a state grant of immunity from liability of custodians "for an act or omission done in good faith in compliance with" UFADAA, but the federal ECPA contains no such immunity.

Fiduciaries are required to provide the custodian (email provider, ISP, social media host, etc.) with certified copies of court documents (such as the fiduciary's lawful appointment), and with original or copies of other documents, including a certification by the fiduciary, and if the custodian does not respond within 60 days the fiduciary may seek a court order directing compliance.

Someone must convince a court to decide whether the custodian is "permitted" to disclose requested content but who will bear that cost: custodian, fiduciary or account holder and given the ambiguities in the ECPA, is it appropriate to force the issue at this point in time?

Once the fiduciary gains access, UFADAA grants certain powers such as control of the digital asset (i.e., the power to move or delete the item), and the power to make a copy of the digital asset (unless prohibited under copyright law -- see also No. 5 of this report). Even this limited "right" to see and control content creates privacy issues.

2. Default/Fallback Rule. Account holders may opt out of the fiduciary access provisions of UFADAA and thereby prohibit their designated fiduciaries from gaining access to digital assets. Opt out procedures differ depending on the nature of the fiduciary, but could include (a) executing a new will or trust containing a provision directing that the fiduciary NOT have access to digital assets, or (b) entering into a separate TOS agreement containing a provision which limits a fiduciary's right to access the digital assets of the account holder.

In order to be enforceable against a fiduciary, a TOS agreement containing restrictions on the fiduciary's right to access digital assets must meet specific requirements. In particular, the account holder must agree to the restrictive provision "by an affirmative act separate from the account holder's assent to other provisions of the agreement". This might require, at a minimum, that the account holder "click through" two separate times, once to approve the restriction on fiduciary access under UFADAA and a

[7] 18 U.S.C. Section 2510 et. seq.

second time to agree to the remaining provisions of the TOS agreement. A TOS that does not meet the requirements is "void as against the strong[8] public policy of this state[9]."

The Committee questions whether UFADAA has selected the correct "default" or "fallback" rule, i.e., does the Act strike the right balance by presuming that the account holder (or the principal under a power of attorney) would have wanted his or her fiduciary to have access to digital assets including email, online profiles, restricted social medial content, etc.?

This presumption may be appropriate for traditional assets such as a bank account, i.e., Washington residents have long known that their fiduciaries will access those accounts. Not all digital assets are traditional, however, and the question is whether the Act should be more nuanced by making the opposite presumption for sensitive non-public information such as social media accounts or "chats" on sensitive topics which used to occur face-to-face or over the telephone in media that did not preserve them. Some " paper mail" has long deliberately been discarded, preserved or hidden -- when the same mail become digital but is protected via passwords or access rights restrictions, is it appropriate to presume that the fiduciary should have access to all of it? This presumption has been criticized by industry groups as encroaching on the privacy rights of the deceased or incapacitated[10]. Committee members made inquiries to colleagues, friends and family members and were interested to learn that most were surprised and offended by the idea that their "private" accounts could be disclosed without their permission and seemed to distinguish between accounts touching on personal, intimate or private information (such as chat room exposing a hidden disease, relationship or sexual orientation that do not inherently need to be known by the fiduciary) and non-personal but confidential accounts (such as bank and stock accounts that are critical to protect and that inherently do need to be known by the fiduciary).

It may be that UFADAA created an "all or nothing" default rule because it would have been too confusing, costly, or inefficient to take a more nuanced approach. Even if so, the question remains whether UFADAA makes the correct choice, i.e., UFADAA has opt-OUT rule instead of an opt-IN rule.

Another approach in an environment in which states will purport to act uniformly by adopting UFADAA, might be to consider multi-state provision of one online mechanism by which account holders could "opt IN" to UFADAA. Custodians finding that unacceptable (e.g., because of compliance costs) could provide notice of account closure or conformance when the account-holder is still alive and capable of finding another custodian, and fiduciaries could consult this "one-stop" source. The devil would be in the details and costs of such a structure, but as noted below, UFADAA currently risks creating surprise and unintended consequences.

3. Choice of Law Confusion; Interstate Commerce Clause Issues. The Act prohibits custodians of digital assets from using a TOS choice of law provision to apply the law of another state in order to restrict fiduciary access to digital assets. Notably, the Act does not limit its applicability to account holders who reside in Washington state or who resided in Washington at the time their digital assets were created or last modified. Nor does it limit applicability to custodians subject to the jurisdiction of Washington state nor to digital assets stored in the state. Instead, it seems to apply to digital assets anywhere in the world created by account

---

[8] The Official Comment to UFADAA explains what is meant by the phrase "strong public policy" but cites Restatement (Second) Conflicts of Laws provisions that have been at least partially rejected by Washington courts. If Washington were to adopt UFADAA, the legislature should review what in Washington is (or is not) meant by "strong" public policy to avoid creating new legal issues under Washington case law and other WA statutes that do not use that phrase.

[9] UFADAA – Section 8(b) (emphasis added)

[10] See discussion at Wills, Trusts & Estates Prof Blog – Friday October 10, 2014 http://lawprofessors.typepad.com/trusts_estates_prof/2014/10/controversy-for-digital-asset-legislation.html

holders anywhere in the world, if a fiduciary of this state has power over that asset. This exercise of extraterritorial jurisdiction may be problematic.

For example, Washington's Personality Rights Act (Chapter 63 RCW) ("WPRA"), as amended, purports to address survivability and assignability of personality rights regardless of the deceased individual's home state. In *Experience Hendrix L.L.C. v. HendrixLicensing.com LTD, 766 F. Supp. 2d 1122 (W.D. Wash. 2011)*, the U.S. District Court for the Western District of Washington declared that the WPRA's choice of law provisions violated the Due Process, Full Faith and Credit, and Commerce Clauses of the U.S. Constitution. The court held that WPRA would apply Washington law in situations where Washington lacked "significant contact" to the events and parties involved, so the statute's choice-of-law provisions were "arbitrary and unfair," and violated the Due Process and Full Faith and Credit Clauses. Moreover, as the WPRA choice-of-law provisions would allow Washington to apply its statutes to commercial transactions taking place outside of the state, they also violated the Commerce Clause. Recently, the Ninth Circuit reversed the ruling of the District Court because the suit filed by Experience Hendrix L.L.C. only related to goods sold within Washington State. Otherwise, the Circuit Court did not criticize the District Court's reliance upon the Due Process and Full Faith and Credit Clauses nor dormant Commerce Clause. In fact, the Circuit Court opined that Washington's approach to post-mortem personality rights raises difficult questions regarding whether another state must recognize the broad personality rights that Washington provides. *Experience Hendrix L.L.C. v. HendrixLicensing.com LTD,* 762 F.3d 829 (9th Cir. 2014).

This issue is further exacerbated by Section 8(c), which provides that:

> (c) A choice-of-law provision in a terms-of-service agreement is unenforceable against a fiduciary acting under this [act] to the extent the provision designates law that enforces a limitation on a fiduciary's access to a digital asset, and the limitation is void under subsection (b).

What result if Washington adopts UFADAA and a Texas account holder creates a Match.com account with a California online service whose TOS adopt California law and includes a privacy policy enforceable under California law; several years later, when leaving for a military assignment overseas, the account holder signs a general power of attorney in favor of his sister, governed by Washington law. Should the sister have access to her brother's Match.com account? Must the California custodian risk violating California law by honoring the demands of the sister in Washington? What result if CA or TX adopt a non-uniform version of UFADAA? Comments to Section 8 of the Act imply that none of this will be problematic but do not mention the interstate commerce clause or other issues.

4. Additional Fiduciary Burdens? Adopting UFADAA may create unintended consequences for fiduciaries and their legal advisors regarding whether the Act creates an obligation or expectation that every fiduciary will or must conduct a search of the account holder's online activities?

An example is RCW 11.42 which requires that personal representatives provide actual notice to creditors of the deceased who are "reasonably ascertainable"[11]. A reasonably ascertainable creditor is defined as one that the notice agent (typically the personal representative or attorney) "would discover upon exercise of reasonable diligence". It was suggested to the Subcommittee that adoption of UFADAA would require amendment of RCW 11.42.040 and that absent such, all personal representatives might feel compelled to carry on a search of the decedent's online activities under UFADAA.

To take the example further, how would a fiduciary find all digital assets given the ubiquity of online accounts, and how would the fiduciary give notice to custodian creditors of the need for them to file a claim against the probate estate? If per No. 4 above Washington takes the position that UFADAA applies to every asset worldwide, must the fiduciary publish notice worldwide in a legal newspaper -- how and at what cost?

[11] RCW 11.42.040

5. New Costs or Reactive Cost Shifting? UFADAA would have unintended consequences. Most custodians are currently handling fiduciary requests as a courtesy (although some states have non-uniform laws regarding same). Once UFADAA is widely adopted, those bound to comply or to bear costs or risks can be expected to react. For example:

- Under § 9 of the Act, a custodian "shall comply" with a fiduciary's request for a copy of the asset "to the extent permitted by copyright law." Making an assessment of whether copyright law allows a copy to be made is much easier said than done and who will bear the cost of an incorrect decision: custodian, fiduciary or account-holder? The Committee agrees that copyright law must be honored, but it is naïve to expect that custodians will necessarily know what that law requires and the article noted at the beginning of this report illustrates that fiduciaries may make improper demands. Consider a custodian cloud provider that has held for several years, a copy of music licensed to an account holder; custodian has not seen and does not want to create a structure to review the licenses governing that copy but assume the fiduciary claims it is entitled to a copy or directs distribution of the copy to an heir? Either the custodian, fiduciary or heir may need a court order -- who pays for that?

- Custodians not having personnel or budget to create a compliance department to process fiduciary requests may best protected by contracting to terminate and deleting data on or soon after the date of death. Account holders seeking to use the custodian as a storage service will contract routinely to make their own back-up copies in case of termination. This would be a legitimate, cost-effective risk avoidance approach to UFADAA compliance obligations, but likely is not an intended result of UFADAA enactment.

- Custodians willing to provide a compliant post-death (or incapacity) service might begin to do so only for a new service fee, including requiring account holders (or their successors) to pay all court costs incurred by the custodian to avoid violation of the ECPA, demands made by intellectual property owners, or concerns about compliance of fiduciary documentation (such as documents that do not allow good faith reliance).

Given that many online account services are free to account holders, it is quite possible that adoption of UFADAA will result in a national bias in favor of deleting digital assets upon the death of account holders or the imposition of fees for a formerly free service. A version of the "deletion" possibility can be seen in the reaction of companies concerned about being required to respond to governmental requests for phone records of their customers. Some of those companies have announced that they will encrypt phone data in order to create an inability to respond to data requests.

6. Probate Codes and Other Related Laws. The procedural requirements of UFADAA may be out-of-step with the reality and business models of the digital world, or at least the portion that is not heavily regulated. The Committee understands the need for a custodian to deal only with a bona fide fiduciary, but if accomplishing that requires online services to establish off-line compliance methods (creating departments to deal with § 9 "certified letters" that appear to require paper letters certified by the US post office) then UFADAA is at odds with their cost and cultural and technology structures. One can speculate that small companies will not be capable of complying (or even know that they must) and that large companies such as Google (Gmail) or Facebook will need to spend considerable sums to comply.

7. Employers. UFADAA should not be adopted until it is amended expressly to exclude employers from the definition of "custodian;" the Act's attempt to exclude employers under § 3(b) is insufficient. Section 3 and several Official Comments intend employers to be excluded, but comments are not part of the law and

courts navigating the literal definitions may conclude that an employer is a "custodian." [12] The Act does not deal with the complexities of employer relationships and ULC comments are based on the false premise that employers do not have "terms of service agreements" with their employees. To the contrary, most employers have email or computer usage policies or agreements the existence and enforceability of which impact critical legal rights and defenses of employers under a variety of laws.

8. Access. As previously noted, the intent of UFADAA is to allow a designated fiduciary to "step into the shoes" of the account holder and exercise no greater rights than the original account holder. There are circumstances, however, when that premise is incorrect. Trade secrets or very private or sensitive information are often protected by law or contracts affording access only to *particular* person, i.e., the account holder who may be trusted by a third party. Access is not appropriate by anyone else, even the trusted person's agent. Fiduciary duties do not solve this because those duties run to the account holder and not to the third person who contracted for access only by the account holder. UFADAA should be amended by the ULC to provide that in those kinds of situations, a custodian may deny access to a fiduciary unless the fiduciary obtains a court order providing sufficient protections (e.g., precluding access by the fiduciary but allowing it to a party trusted by the third party, posting of a bond, or having only the court see the information under seal).

9. Intellectual Property. UFADAA notes that its rules are subject to federal intellectual property law. Section 9(g), however, is puzzling and creates a question whether it creates a bona fide transferee defense for "persons" who in good faith entered into a transaction in reliance on a trustee's certification regarding the trustee's powers. There is no Official Comment explaining what the subsection means.

Assume an account holder is the licensee of a digital book that may not be copied or transferred under copyright law or the contract; the custodian of the book does not know copyright law so makes and transmits a copy to a trustee under § 9(a) in reliance on the trustee's §9(d) certification. The trustee distributes or sells the copy under the trust. Is the recipient of the copy a "person" protected by § 9(g)? If that is a possibility, UFADAA conflicts with intellectual property laws (i.e., there is no bona fide purchaser defense). Would the custodian, trustee and recipient potentially be liable for infringement (direct, contributory or vicarious), all as encouraged by UFADAA or ambiguity regarding the purpose of § 9(g)?

D. What timing concerns does UFADAA create?

1. Is there a current need for this statute – are fiduciaries presently unable to satisfactorily perform their obligations and to administer digital assets? Committee members are aware of situations where fiduciaries have found it challenging to search for unknown on-line bank or brokerage accounts or other financial assets. However, trust and estates attorneys polled by the subcommittee's members indicated that

---

[12] See UFADAA Official Comment to Sec. 2 (false premises are bolded) ("A **custodian includes any Internet service provider** as well as any other entity that provides or stores electronic data of an account holder. **A custodian does not include most employers because an employer typically does not have a terms-of-service agreement with an employee.**). *See also* comments to Sec. 3, Example 1 (false premise is bolded):

> Example 1—Fiduciary access to an employee e-mail account. D dies, employed by Company Y. Company Y has an internal e-mail communication system, available only to Y's employees, and used by them in the ordinary course of Y's business. D's personal representative, R, believes that D used Company Y's e-mail system to effectuate some financial transactions that R cannot find through other means. R requests access from Company Y to the e-mails.
>
> Company Y is not a custodian subject to the act. Under Section 2(7), a custodian must carry, maintain or store an account holder's digital assets. An account holder, in turn, is defined under Section 2(1) as someone who has entered into a terms-of-service agreement. **Company Y, like most employers, did not enter into a terms-of-service agreement with D, so D was not an account holder**.

where there was a need, they were able to gain access digital assets and to properly resolve associated probate issues. The subcommittee believes that it may be possible to address this issue without adopting a statute creating the types of problems noted above.

2. What advantage is there to Washington in being an "early adopter" of UFADAA? Would Washington be better off delaying consideration until the operation of the Act can be observed? Online services providers who violate the federal ECPA can potentially be sued for significant statutory damages and attorney's fees by third parties whose email or other electronic communications may be stored in a decedent's email account and released without appropriate third party permission[13]. Also of concern for a custodian are violations of federal intellectual property laws or Federal Trade Commission unfair acts or deceptive practice principles for privacy policies made before or without knowledge of UFADAA (e.g., policy for sexual orientation site commits to privacy but UFADAA allows account holder's family member fiduciary access). Of concern to account holders is the UFADAA default rule that presumes it is fine for the fiduciary to see everything -- the Act allows the account holder to opt-out, but most account holders will not realize that or take the time separately to accomplish it (they may still assume that something so private would not be the subject of such a default rule).

Given the uncertainty as to how UFADAA will interplay with federal or other laws, the Committee is concerned that adoption of UFADAA may expose online service providers to unnecessary legal risk or claims. Further, several years from now, Congress might respond to requests for updating the ECPA and create a uniform nationwide regime completely different from UFADAA, in which case, courts would be faced with deciding which aspects of UFADAA to continue to enforce and state legislatures might be best served by repealing UFADAA.

E. The Law of Commerce in Cyberspace Committee and its work

A list of the Committee's general membership is attached. While all members were provided the opportunity to participate in the review, not all were able to participate. The work was led by a subcommittee whose members solicited and received input from other Committee members or members of the probate bar. The subcommittee considered the proposed statutory language of UFADAA as well as the Official Comments provided by the ULC in regard to the interpretation and operation of the Act. The subcommittee also considered various working papers and third-party comments as located at the ULC web site (http://www.uniformlawcommission.com/Committee.aspx?title=Fiduciary Access to Digital Assets). Before finalizing this Report, a draft was shared with the Chairs of the WSBA Real Property Probate & Trust Section, Probate & Trust Council, and Elder Law Section, and input was sought from them. Among the guiding principles used by the Committee were the following:

1. The Committee is a part of the WSBA Business Section which is concerned with the promotion and impact of legislation on Washington businesses, commerce and individuals.

2. The role of the bar is to serve as an educational vehicle for the legislature and to review proposed legislation from all perspectives, including small and large parties to consumer and business affairs, transactions or contracts. Committee members endeavored to leave any client hats at the door.

3. The Committee adopted the premise that extra burdens should not be placed on electronic transactions or affairs simply because they are electronic.

---

[13] Letter dated July 8, 2013 – State Privacy and Security Coalition, Inc. sent to Suzanne Brown Walsh c/o ULC. http://www.uniformlawcommission.com/Committee.aspx?title=Fiduciary Access to Digital Assets

Washington Bar Association Business Law Section Committee on the Law of Commerce in Cyberspace

Subcommittee: Alex Modelski, Greg Dennis and Scott Warner

Chair of Committee: Holly K. Towle

Committee Roster:

CLCC Member

John R. Christiansen Christiansen IT Law	Brian P. McClatchey K&L Gates LLP 618 W. Riverside Avenue, Suite 300 Spokane, WA 99201
Teresa Daggett Gordon Thomas & Honeywell 600 University, Suite 2100 Seattle, WA 98101	Ken Moyle DocuSign 1301 2nd Avenue, Suite 2000 Seattle, WA 98101
Gregory J. Dennis Landerholm P.S. 805 Broadway, Suite 1000 Vancouver, WA 98660	Anita Ramasastry Assistant Professor of Law Associate Director, Center for Law, Commerce and Technology University of Washington School of Law 1100 NE Campus Parkway Seattle, WA 98105
Tolis Dimopoulos Sophos Law Firm, PLLC	Mark Sanders EchoSign Product Counsel Adobe Legal Department 801 N. 34th Street Seattle, WA 98103
Roger Hawkes Hawkes Law Firm P.S. 19929 Ballinger Way NE, Suite 200 Shoreline, WA 98155	Geana M. Van Dessel Witherspoon Kelley 422 W. Riverside Avenue, Suite 1100 Spokane, WA 99201
Erin Joyce Letey Riddell Williams 1001 Fourth Avenue, Suite 4500 Seattle, WA 98154	Mark Wittow K&L Gates 925 Fourth Avenue, Suite 2900 Seattle, WA 98104
Selina Koonar B.A, J.D., L.L.M. Candidate	Holly Towle K&L Gates LLP 925 Fourth Avenue, Suite 2900 Seattle, WA 98104
Danan G. Margason Reed Longyear Malnati & Ahrens 1415 Norton Building 801 Second Avenue Seattle, WA 98104	cc only (not committee member): Gwen Lloyd Legislative Assistant Washington State Bar Association 111 21st Avenue SW Suite 1-B Olympia, WA 98501
Alex Modelski ATER WYNNE LLP | 601 Union Street, Suite 1501 | Seattle, WA 98101	