

D R A F T
FOR DISCUSSION ONLY

FIDUCIARY ACCESS TO DIGITAL ASSETS ACT

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

MEETING IN ITS ONE-HUNDRED-AND-TWENTY-SECOND YEAR
BOSTON, MASSACHUSETTS
JULY 6 - JULY 12, 2013

FIDUCIARY ACCESS TO DIGITAL ASSETS ACT

WITH PREFATORY NOTE AND COMMENTS

Copyright ©2013
By
NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the Drafting Committee. They do not necessarily reflect the views of the Conference and its Commissioners and the Drafting Committee and its Members and Reporter. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

May 31, 2013

DRAFTING COMMITTEE ON FIDUCIARY ACCESS TO DIGITAL ASSETS ACT

The Committee appointed by and representing the National Conference of Commissioners on Uniform State Laws in preparing this act consists of the following individuals:

SUZANNE BROWN WALSH, P.O. Box 271820, West Hartford, CT 06127, *Chair*

DAVID BIKLEN, 799 Prospect Ave., West Hartford, CT 06105

STEPHEN CHOW, 125 Summer St., Boston, MA 02110-1624

VINCE DELIBERATO, JR., Legislative Reference Bureau, Main Capitol Bldg., Harrisburg,
PA 17120-0033

MARC FEINSTEIN, 431 N. Phillips Ave., Suite 301, Sioux Falls, SD 57104

GENE HENNIG, 500 IDS Center, 80 S. 8th St., Minneapolis, MN 55402-3796

STAN KENT, 90 S. Cascade Ave., Suite 1210, Colorado Springs, CO 80903

SUSAN KELLY NICHOLS, North Carolina Dept. of Justice, P.O. Box 629, Raleigh,
NC 27602-0629

DAN ROBBINS, 15301 Ventura Blvd., Bldg. E, Sherman Oaks, CA 91403

LANE SHETTERLY, 189 S.W. Academy St., P.O. Box 105, Dallas, OR 97338

NAOMI CAHN, George Washington University School of Law, 2000 H St. NW, Washington,
DC 20052, *Reporter*

EX OFFICIO

MICHAEL HOUGHTON, P.O. Box 1347, 1201 N. Market St., 18th Floor, Wilmington,
DE 19899, *President*

GAIL HAGERTY, South Central Judicial District, P.O. Box 1013, 514 E. Thayer Ave.,
Bismarck, ND 58502-1013, *Division Chair*

AMERICAN BAR ASSOCIATION ADVISOR

KARIN PRANGLEY, 500 N. Dearborn St., Suite 200, Chicago, IL 60654-3372, *ABA Advisor*

VICKI LEVY ESKIN, 1732 N. Ronald Reagan Blvd., Longwood, FL 32750-3409,
ABA Section Advisor

CHRISTINA KUNZ, William Mitchell College of Law, 875 Summit Ave., St. Paul, MN 55105,
ABA Section Advisor

DAVID SHULMAN, 401 E. Las Olas Blvd., Suite 130-491, Fort Lauderdale, FL 33301-2210,
ABA Section Advisor

EXECUTIVE DIRECTOR

JOHN A. SEBERT, 111 N. Wabash Ave., Suite 1010, Chicago, IL 60602, *Executive Director*

Copies of this act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
111 N. Wabash Ave., Suite 1010
Chicago, Illinois 60602
312/450-6600
www.uniformlaws.org

FIDUCIARY ACCESS TO DIGITAL ASSETS ACT

TABLE OF CONTENTS

SECTION 1. SHORT TITLE	1
SECTION 2. DEFINITIONS.....	1
SECTION 3. FIDUCIARY AUTHORITY.....	4
SECTION 4. CONTROL OF DIGITAL PROPERTY AND ACCESS TO COMMUNICATIONS OF DECEDENT BY PERSONAL REPRESENTATIVE.....	6
SECTION 4. AUTHORITY OVER DIGITAL PROPERTY OF DECEDENT BY PERSONAL REPRESENTATIVE	7
SECTION 5. CONTROL OF DIGITAL PROPERTY AND ACCESS TO COMMUNICATIONS OF PROTECTED PERSON BY [CONSERVATOR].....	8
SECTION 5. AUTHORITY OVER DIGITAL PROPERTY OF PROTECTED PERSON BY [CONSERVATOR].....	8
SECTION 6. CONTROL OF DIGITAL PROPERTY BY AGENT UNDER POWER OF ATTORNEY	10
SECTION 7. CONTROL OF DIGITAL PROPERTY BY TRUSTEE.....	10
SECTION 8. DIGITAL PROPERTY RECOVERY FROM CUSTODIAN	11
SECTION 9. CUSTODIAN IMMUNITY	13
SECTION 10. UNIFORMITY OF APPLICATION AND CONSTRUCTION.....	13
SECTION 11. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT	13
[SECTION 12. SEVERABILITY	14
SECTION 13. APPLICABILITY	14
SECTION 14. REPEALS; CONFORMING AMENDMENTS	14
SECTION 15. EFFECTIVE DATE.....	14

FIDUCIARY ACCESS TO DIGITAL ASSETS ACT

Prefatory Note for the Drafting Committee

The purpose of this act is to vest fiduciaries with the authority to access, manage, distribute, copy or delete digital assets and accounts. It addresses four different types of fiduciaries: personal representatives of decedents' estates, conservators for protected persons, agents acting pursuant to a power of attorney, and trustees.

As the number of digital assets held by the average person increases, questions surrounding the disposition of these assets upon the individual's death or incapacity are becoming more common. Few laws exist on the rights of fiduciaries over digital assets. Few holders of digital assets and accounts consider the fate of their online presences once they are no longer able to manage their assets. And these assets have real value: according to a 2011 survey from McAfee, Intel's security-technology unit, American consumers valued their digital assets, on average, at almost \$55,000.¹ These assets range from online gaming pieces to photos, to digital music, to client lists, to bank accounts, to bill-paying, etc. There are 30 million Facebook accounts that belong to dead people.² The average individual has 25 passwords. Some service providers have explicit policies on what will happen when an individual dies, others do not;³ even where these policies are included in the terms of service, most consumers click-through these agreements.

Only a minority of states have enacted legislation on fiduciary access to digital assets: Connecticut, Idaho, Indiana, Oklahoma, and Rhode Island. In addition, other states, including Massachusetts, Nebraska, New York, and Oregon, have considered, or are considering, legislation.⁴ Existing legislation differs with respect to the types of digital assets covered, the rights of the fiduciary, and whether the principal's death or incapacity is covered.

This draft is for review by the Drafting Committee. While an earlier draft focused on amendments to existing uniform laws in this area, this draft is designed to be a stand-alone act. The draft is divided into eleven sections. Sections 1-3 contain general provisions and definitions, including those relating to the scope of the fiduciary's authority. Sections 4-7 establish the rights of personal representatives, conservators, agents acting pursuant to a power of attorney, and trustees. Section 8 contains provisions relating to the rights of the fiduciary to recover property. Section 9 addresses relief from liability for compliance. Sections 10-14 address miscellaneous issues, including the effective date of the act and similar issues.

¹ Kelly Greene, *Passing Down Digital Assets*, WALL STREET JOURNAL (Aug. 31, 2012, 8:20 PM), <http://online.wsj.com/article/SB10000872396390443713704577601524091363102.html>.

² Craig Blaha, *Over 30 Million Accounts on Facebook Belong to Dead People*, TECHNORATI (March 7, 2012, 11:05 AM), <http://technorati.com/technology/article/over-30-million-accounts-on-facebook>.

³ For a concise listing, see, e.g., DECEASED ACCOUNT, <http://deceasedaccount.com> (last visited Nov. 7, 2012).

⁴ A memo summarizing these laws and legislative proposals is available on the shared Google Drive.

After many of the proposed sections, a Comment to the Committee discusses the drafting of the section and raises issues for Committee consideration. The Comments should be read in conjunction with the proposed statutory text. Some of the major issues for Committee consideration include:

1 **FIDUCIARY ACCESS TO DIGITAL ASSETS ACT**

2 **SECTION 1. SHORT TITLE.** This [act] may be cited as the Fiduciary Access to

3 Digital Assets Act.

4 **SECTION 2. DEFINITIONS.** In this [act]:

5 (1) “Account holder” means a person, including a decedent, that has entered into a
6 terms-of-service agreement.

7 (2) “Agent” means an attorney-in-fact granted authority under a durable or nondurable
8 power of attorney.

9 (3) “[Conservator]” means a person that is appointed by a court to manage the estate of
10 an individual. The term includes a limited [conservator].

11 [(4) “Contents,” when used in connection with an electronic communication, means
12 information concerning the substance, purport, or meaning of the communication.]

13 (5) “[Court” means the [insert name of court in this state having jurisdiction in matters
14 relating to the content of this [act]].

15 (6) “Custodian” means a person that stores, or has control of, digital property or
16 electronic communication of an account holder.

17 (7) “Digital account” means an electronic system for creating, generating, sending,
18 receiving, storing, displaying, or processing information to which the account holder has access.

19 (8) “Digital asset” means information created, generated, sent, communicated, received,
20 or stored by electronic means on a digital device or system that delivers digital information. The
21 term includes a contract right.

22 (9) “Digital device” means an electronic device that can receive, store, process, or send
23 digital information.

1 (10) “Digital property” means the lawful ownership and management of and rights
2 related to a digital account and digital asset. [The term does not include the contents of an
3 electronic communication.]

4 (11) “Electronic” means relating to technology having electrical, digital, magnetic,
5 wireless, optical, electromagnetic, or similar capabilities.

6 (12) “Electronic communication” means a transfer of a sign, signal, writing, image,
7 sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,
8 electromagnetic, photoelectronic or photooptical system that affects interstate or foreign
9 commerce. The term does not include a wire or oral communication; any communication made
10 through a tone-only paging device; any communication from a tracking device; or electronic
11 funds transfer information stored by a financial institution in a communications system used for
12 the electronic storage and transfer of funds.

13 (13) “Electronic communication service” means a person that provides electronic
14 communications to the public.

15 (14) “Fiduciary” includes a personal representative, [conservator], guardian, agent, or
16 trustee.

17 (15) “Governing instrument” means a will, trust, instrument creating a power of attorney,
18 or trust or other dispositive or nominative instrument.

19 (16) “Information” means data, text, images, sounds, codes, computer programs,
20 software, databases or similar intelligence of any nature.

21 (17) “Person” means an individual, estate, business or nonprofit entity, public
22 corporation, government or governmental subdivision, agency, or instrumentality, or other legal
23 entity.

1 (18) “Personal representative” means an executor, administrator, successor personal
2 representative, special administrator, or a person that performs substantially the same function
3 under law of this state other than this [act].

4 [(19) “Power of attorney” means a record that grants an agent authority to act in the place
5 of a principal with respect to digital property.]

6 (20) “Principal” means an individual who grants authority to an agent in a power of
7 attorney.

8 (21) “Protected person” means an individual for whom a protective order has been
9 entered.

10 (22) “Protective order” means an order appointing a [conservator] or related to
11 management of a protected person’s digital property.

12 (23) “Record” means information that is inscribed on a tangible medium or that is stored
13 in an electronic or other medium and is retrievable in perceivable form.

14 (24) “Remote computing service” means a person that stores electronic records or
15 provides computer processing services to the public by means of an electronic communication
16 service.

17 (25) “Terms-of-service agreement” means an agreement that controls the relationship
18 between an account holder and a custodian. The term includes a terms-of-use agreement, a
19 license agreement, and a privacy policy.

20 (26) “Trustee” means a fiduciary with legal title to assets pursuant to an agreement or
21 declaration that creates a beneficial interest in others.

22 (27) “Will” means a testamentary instrument. The term includes a codicil and a
23 testamentary instrument that only appoints an [executor] or revokes or revises another will.

Comments for the Committee

The definitions of agent, conservator, court, electronic, fiduciary, governing instrument, information, person, personal representative, power of attorney, principal, property, protected person, protective order, record, and will are based on those in the Uniform Probate Code. The other definitions are new for this act, although the definition of digital service comes from the White House Digital Government Strategy:

<http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf>. The definition of “contents” is taken from 18 U.S.C. § 2510(8), the definition of “electronic communication” tracks the language of 18 U.S.C. § 2510(12), the definition of “electronic communication service” is drawn from 18 U.S.C. 2510(15), and the definition of “remote computing service” is adapted from 18 U.S.C. § 2711(2), to help ensure the Act’s compliance with federal law.

A custodian does not include an employer because an employer typically does not have a terms-of-service agreement with an employee. Any digital property created through employment generally belongs to the employer.

SECTION 3. FIDUCIARY AUTHORITY.

(a) This [act] applies only to a grant of authority to a fiduciary.

(b) A fiduciary with [legal] authority over digital property of an account holder has the authority as the account holder. The exercise of authority by a fiduciary over digital property is not a transfer of the property. The rights of the account holder are subject to copyright law as well as any applicable and enforceable terms of service agreement.

(c) A fiduciary with authority over digital property of an account holder has the lawful right of the account holder and is an authorized user of the account.

(d) A fiduciary with authority over a digital device of a decedent, protected person, ward, or settlor may access any record stored on the digital device.

Comment

This section distinguishes the authority of fiduciaries over digital property subject to this act from any other efforts to access the digital property. Family members or friends may seek access to the digital property of others, but such efforts are subject to other laws and are not covered by this act. Moreover, the fiduciary exercises authority only on behalf of the account holder.

Subsection (b) clarifies that the fiduciary has the same authority as the account holder.

1 This issue potentially arises in two situations: 1) the fiduciary obtains access to a password
2 directly from the account holder, as would be true in various circumstances such as for the
3 trustee of a trust or someone who has stored passwords with a digital locker; and 2) the fiduciary
4 has obtained access pursuant to this act. The fiduciary does not, however, obtain power over any
5 digital property if that property was illegally obtained by the account holder. The section also
6 provides that control by a fiduciary should not be considered a transfer that would violate the
7 anti-transfer terms of a terms-of-service agreement.

8 Subsection (c) is designed to establish that the fiduciary is authorized to exercise control
9 over digital property in accordance with other applicable laws. The language mirrors that used in
10 Title II of the Electronic Communications Privacy Act of 1986 (ECPA), known as the Stored
11 Communications Act (SCA), 18 U.S.C. § 2701 *et seq.* The subsection clarifies that the fiduciary
12 is “authorized” under the two federal statutes that prohibit unauthorized access to computers and
13 computer data, the SCA and the Computer Fraud and Abuse Act,⁵ as well as pursuant to any
14 comparable state laws criminalizing unauthorized access.⁶

15 The Stored Communications Act contains two potentially relevant prohibitions.

16 1) 18 U.S.C. § 2701(a), which concerns access to the digital property, makes it a crime
17 for anyone to “intentionally access [] without authorization a facility through which an electronic
18 communication service is provided” as well as to “intentionally exceed [] an authorization to
19 access that facility.” Thus, someone who has authorization to access the facility is not engaging
20 in criminal behavior. Moreover, this section does not apply to “conduct authorized . . . by a user
21 of that service with respect to a communication of or intended for that user.”⁷

22 2) 18 U.S.C. § 2702, “Voluntary disclosure of customer communications or records,”
23 concerns actions by the service provider. It prohibits an electronic communication service or a
24 remote computing service from knowingly divulging the contents of a communication that is
25 stored by or carried or maintained on that service unless disclosure is made (among other
26 exceptions) “to an addressee or intended recipient of such communication or an agent of such
27 addressee or intended recipient” or “with the *lawful consent* of the originator or an addressee or
28 intended recipient of such communication, or the subscriber in the case of remote computing
29 service.” 18 U.S.C. § 2702(b)(1), (3) (emphasis added). The statute permits disclosure of
30 “customer records” that do not include content, either with lawful consent from the customer or
31 “to any person other than a governmental entity.” 18 U.S.C. § 2702(c)(2) and (6). Thus, unlike
32 the contents, the provider is permitted to disclose the non-content “records” of the electronic

⁵ Stored Communications Act, 18 U.S.C. § 2701 *et seq.* (2006); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* (2006); *see, e.g.*, Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004); Allan D. Hankins, Note, *Compelling Disclosure of Facebook Content Under the Stored Communications Act*, 17 SUFFOLK J. TRIAL & APP. ADVOC. 295 (2012).

⁶ *See Computerized Hacking and Unauthorized Access States Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 21, 2009), <http://www.ncsl.org/issues-research/telecom/computer-hacking-and-unauthorized-access-laws.aspx>; Christina Kunz, Peter Rademacher & Lucie O’Neill, 50 State Survey of Unauthorized Access (2012) (on file with the Committee and available on the Google Drive).

⁷ 18 U.S.C. §§ 2701(a), (c)(2).

communications to anyone except the government, and may disclose to the government with the customer's lawful consent or in certain emergencies.

The Computer Fraud and Abuse Act (CFAA) prohibits unauthorized access to computers. 18 U.S.C. § 1030. Like the SCA, the CFAA similarly protects against anyone who “intentionally accesses a computer without authorization or exceeds authorized access.” 18 U.S.C. § 1030(a).

6 State laws vary in their coverage, but typically prohibit unauthorized access.

7 By defining the fiduciary as an authorized user: 1) the fiduciary has authorization to
8 access the files under the *first* section of the SCA, 18 U.S.C. § 2701, as well as under the CFAA;
9 and 2) the fiduciary has “the lawful consent” of the originator/subscriber so that the provider can
10 voluntarily disclose the files pursuant to the *second* relevant provision of the SCA, 18 U.S.C.
11 § 2702. Moreover, this language should be adequate to avoid liability under the state
12 unauthorized access laws.

13 Subsection (d) is designed to clarify that the fiduciary is authorized to access material
14 stored on the digital device of the decedent, protected person, principal, or settlor, thereby
15 superseding state laws on unauthorized access to the device.

Alternative A

SECTION 4. CONTROL OF DIGITAL PROPERTY AND ACCESS TO

18 **COMMUNICATIONS OF DECEDENT BY PERSONAL REPRESENTATIVE.** Except as
19 a decedent otherwise provided by will or unless otherwise prohibited by a court, and subject to
20 Section 3, a personal representative may:

21 (1) exercise control over digital property of the decedent;

22 (2) to the extent not inconsistent with 18 U.S.C. Section 2702(b)(3), obtain access to the
23 contents of each record controlled by an electronic communication service or a remote
24 computing service sent to or received by the decedent; and

25 (3) obtain other records of the decedent controlled by an electronic communication
26 service or a remote computing service, including a log of the electronic address of each party
27 with whom the decedent communicated.

Alternative B

1 **SECTION 4. AUTHORITY OVER DIGITAL PROPERTY OF DECEDENT BY**

2 **PERSONAL REPRESENTATIVE.**

3 (a) Subject to Section 3 and except as otherwise provided in subsection (b), a personal
4 representative may access, manage, deactivate, and delete the digital property of the decedent.

5 (b) A personal representative may not exercise authority over digital property of a
6 decedent if prohibited by:

- 7 (1) the will of the decedent;
- 8 (2) a court order; or
- 9 (3) law of this state other than this [act].

10 **End of Alternatives**

11 **Comments for the Committee**

12 The Committee has included two different versions of Section 4. The first version
13 responds to the concerns of internet service providers who believe that the act should be
14 structured to clarify the difference between fiduciary authority over digital property other than
15 electronic communications protected by federal law (the Electronic Communications Privacy Act
16 (ECPA)), and authority over ECPA-covered electronic communications. For electronic
17 communications, the Committee had agreed that this next draft would set out procedures that
18 cover: first, logs and records that providers may release without consent under ECPA; and
19 second, ECPA-covered communications. As detailed in the comments to Section 3 (above),
20 federal law distinguishes between the permissible disclosure of the “contents” of a
21 communication, covered in 18 U.S.C. § 2702(b), and of “a record or other information pertaining
22 to a” subscriber or customer, covered in 18 U.S.C. § 2702(c). The first, content-based material,
23 can be divided into two types of communications: those received by the account holder and
24 those sent. Material when the account holder is the “addressee or intended recipient” can be
25 disclosed either to that individual or to an agent for that person. 18 U.S.C. § 2702(b)(1).
26 Material for which the account holder is the “originator” (as well as an addressee or intended
27 recipient) can be disclosed with the account holder’s “lawful consent.” 18 U.S.C. § 2702(b)(3).
28 (Note that, when the account holder is the addressee or intended recipient, material can be
29 disclosed under either (b)(1) or (b)(3), but that when the account holder is the originator, lawful
30 consent is required. By contrast to content-based material, non-content material can be disclosed
31 not only with the lawful consent of the account holder but also to any person other than a
32 governmental entity (which would presumably include fiduciaries)).

33 The second version of Section 4 establishes the default rule that the personal

1 representative is authorized to administer all of the decedent's digital property, regardless of
2 whether it is covered by ECPA. The section is modeled on the formulation of the personal
3 representative's default power set out in UPC Sec. 3-715. The basis for this authority over all
4 digital property is that, under Section 3, the personal representative is deemed to have the lawful
5 consent of the decedent and to be an authorized user so that ECPA would not prevent fiduciary
6 access.

Comment

The term, “otherwise provided by will,” is intended to indicate that a will controls the personal representative’s authority. As is true more generally with respect to interpretation of wills, public policy can override the explicit terms of a will.

Alternative A

SECTION 5. CONTROL OF DIGITAL PROPERTY AND ACCESS TO

13 **COMMUNICATIONS OF PROTECTED PERSON BY [CONSERVATOR].** Subject to
14 Section 3, at the initial hearing on an application to appoint a [conservator] for an individual or
15 on later application by a [conservator] of a protected person, a court may authorize a
16 [conservator] to:

- (1) exercise control over digital property of the individual or protected person;
 - (2) to the extent not inconsistent with 18 U.S.C. Section 2702(b)(3), obtain access to the contents of each record controlled by an electronic communication service or a remote computing service sent to or received by the individual or protected person; and
 - (3) obtain other records of the individual or protected person controlled by an electronic communication service or a remote computing service, including a log of the electronic address of any party with whom the individual or protected person communicated.

Alternative B

SECTION 5. AUTHORITY OVER DIGITAL PROPERTY OF PROTECTED PERSON BY [CONSERVATOR].

- (a) Subject to Section 3, at the initial hearing on an application to appoint a [conservator]

1 for an individual or on later application by a [conservator] of a protected person, the court may
2 authorize the [conservator] to access, manage, deactivate or delete the digital property of the
3 individual or protected person.

4 (b) In granting authority to a [conservator] under subsection (a), the court shall consider
5 intent of the protected person with respect to the authority granted to the extent that intent can be
6 ascertained.

7 **End of Alternatives**

8 **Comments for the Committee**

9 Section 5 establishes that the conservator must be specifically authorized by the court to
10 access the protected person's digital property. Each of the different levels of access must be
11 specifically granted by court order. The Committee may need to clarify that the requirement in
12 Section 5 for express authority over digital property does not limit the fiduciary's authority over
13 the underlying "bricks and mortar" asset, such as a bank account.

14 The two versions of Section 5 are comparable to the two versions of Section 4. The first
15 version responds to the concerns of internet service providers who believe that the act should be
16 structured to clarify the difference between fiduciary authority over digital property other than
17 electronic communications protected by federal law, the Electronic Communications Privacy
18 Act (ECPA), and authority over ECPA-protected electronic communications. For electronic
19 communications, the Committee had agreed that this next draft would set out procedures that
20 cover: first, logs and records that providers may release without consent under ECPA; and
21 second, ECPA-covered communications.

22 In the second version, the conservator is authorized to access all digital property of the
23 protected person, regardless of whether it is ECPA-covered. The basis for this authority over all
24 digital property is that, under Section 3, the conservator is deemed to have the lawful consent of
25 the protected person and to be an authorized user so that ECPA would not prevent fiduciary
26 access.

27 Subsection (b) of the second version repeats the introductory language in UPC
28 Section 5-411(c), and is designed to clarify that a decision by the court to grant powers to the
29 conservator under this section must be based primarily on the decision that the protected person
30 would have made, if of full capacity. The protected person's personal values and expressed
31 desires, past and present, are to be considered when making decisions about the conservator's
32 authority. Existing state law may also set out the requisite standards for a conservator's actions,
33 and the bracketed language allows for reference to those laws. Under Section 3, the conservator
34 has the same power over digital property as the account holder. The conservator must exercise
35 authority in the interests of the protected person.

1 **SECTION 6. CONTROL OF DIGITAL PROPERTY BY AGENT UNDER**

2 **POWER OF ATTORNEY.** Subject to Section 3 of this act, if a power of attorney grants
3 authority to an agent over digital property of a principal, and exercise of the authority is not
4 otherwise prohibited by a governing instrument, the agent may[:]

- 5 (1)] access, manage, deactivate, and delete the property[; and
6 (2) change a governing instrument affecting the property].

7 **Comments for the Committee**

8 This section establishes that the agent must be specifically authorized by the principal to
9 access the principal's digital property, and it is modeled on UPC Sec. 5B-201(a). The American
10 College of Trusts and Estates Counsel's State Laws Committee recently asked the Committee to
11 consider whether the authority should be a default power, instead.

12 Each of the different levels of access must be specifically granted by the power. An
13 affirmative grant of authority to an agent is required because of the risk those acts pose to the
14 principal's property and estate plan, and it is consistent with the agent's lack of supervision by a
15 court.

16 Subsection 2 is bracketed to indicate each state will need to decide whether an agent can
17 change a governing instrument. Because of the danger of fraud and influence inherent in the use
18 of powers of attorney, we may want to discuss further whether or not an agent's control should
19 differ from that granted to other fiduciaries.

20 There should be no question that an explicit delegation of authority in a power of attorney
21 constitutes authorization from the account holder to access digital property, and provides "lawful
22 consent" to allow disclosure of electronic communications from an electronic communications
23 service or a remote computing service pursuant to applicable law. Both authorization and lawful
24 consent are important because 18 U.S.C. § 2701 deals with intentional access without
25 authorization and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

26 **SECTION 7. CONTROL OF DIGITAL PROPERTY BY TRUSTEE.** Subject to

27 Section 3, a trustee may access, manage, deactivate, and delete digital property held in the trust
28 in accordance with the terms of the trust.

29 **Comments for the Committee**

30 There should be no question that holding property in trust constitutes authorization
31 from the account holder to access digital property, and that it provides "lawful consent" to allow
32 disclosure of electronic communications from an electronic communications service or a remote

1 computing service pursuant to applicable law. Both authorization and lawful consent are
2 important because 18 U.S.C. § 2701 deals with intentional access without authorization, and
3 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

4 **SECTION 8. DIGITAL PROPERTY RECOVERY FROM CUSTODIAN.**

5 (a) “Certified copy of a power of attorney” means a record accompanied by an affidavit
6 in which the affiant attests that the record is an accurate record of the original of the power and
7 that, to the best of the affiant’s knowledge, the power remains in effect.

8 (b) If the fiduciary of an account holder complies with subsection (c) and makes a request
9 in a record to a custodian of digital property or electronic communications of the account holder
10 for access to the property and communications [, other than the contents of the communications]
11 or ownership or a copy of the property or communications, the custodian shall comply with the
12 request.

13 (c) If a request under subsection (b) is made:

14 (1) by a personal representative, the request must be accompanied by a certified
15 copy of the letter of appointment of the representative;

16 (2) by a [conservator], the request must be accompanied by a certified copy of the
17 court order that gives the [conservator] authority over the digital property;

18 (3) by an agent, the request must be accompanied by a certified copy of the power
19 of attorney that authorizes the agent to exercise authority over the digital property; or

20 (4) by a trustee, the request must be accompanied by a certified copy of the trust
21 instrument [pursuant to Uniform Trust Code Section 1013] that authorizes the trustee to exercise
22 authority over the digital property.

23 (d) A custodian shall comply with a request made under subsection (b) not later than
24 [60] days after receipt of the request. If the custodian fails to comply, the fiduciary may apply to
25 the court for an order directing compliance.

1 [(e) Instead of furnishing a copy of a trust instrument under subsection (c)(4), the trustee

2 may furnish a certification of trust. A certification of trust:

3 (1) must contain the following information:

4 (A) that the trust exists and the date the trust instrument was executed;

5 (B) the identity of the settlor;

6 (C) the identity and address of the currently acting trustee;

7 (D) the powers of the trustee;

8 (E) the revocability or irrevocability of the trust and the identity of any

9 person holding a power to revoke the trust;

10 (F) the authority of a co-trustee to sign or otherwise authenticate, and

11 whether all or less than all co-trustees are required to exercise powers of the trustee;

12 (G) the trust's taxpayer identification number; and

13 (H) the manner of taking title to trust property;

14 (2) may be signed or otherwise authenticated by any trustee;

15 (3) must state that the trust has not been revoked, modified or amended in a

16 manner that would cause the representations contained in the certification of trust to be incorrect;

17 and

18 (4) need not contain the dispositive terms of a trust.

19 (f) A recipient of a certification of trust under subsection (e) may require the trustee to

20 furnish copies of excerpts from the original trust instrument and later amendments which

21 designate the trustee and confer on the trustee the power to act in the pending transaction.

22 (g) A custodian that acts in reliance on a certification under subsection (e) without

23 knowledge that the representations contained in it are incorrect is not liable to any person for so

1 acting and may assume without inquiry the existence of the facts contained in the certification.

(h) A person that in good faith enters a transaction in reliance on a certification of trust under subsection (e) may enforce the transaction against the trust property as if the representations contained in the certification were correct.

5 (i) A person that demands the trust instrument in addition to a certification of trust under
6 subsection (e) or excerpts under subsection (f) is liable for damages if the court determines that
7 the person did not act in good faith in demanding the trust instrument.]

(j) This section does not limit the right of a person to obtain a copy of a trust instrument in a judicial proceeding concerning the trust.

Comment

11 The bracketed material allows states that have already enacted the UTC to use the shorter
12 version. Those states that have not adopted the UTC may choose to include the bracketed
13 material, which is a slight modification of the language in Uniform Trust Code Section 1013.

Under subsection (d), the custodian must comply within a certain period of time. The Committee may want to discuss, at Style's suggestion, whether to include an expedited time period.

17 **SECTION 9. CUSTODIAN IMMUNITY.** A custodian and its officers, employees,
18 and agents are immune from liability for any action done in compliance with this [act].

Comment

This section establishes that custodians are protected from liability when they act in accordance with the procedures of this act and in good faith. The types of actions covered include disclosure as well as transfer of copies.

23 **SECTION 10. UNIFORMITY OF APPLICATION AND CONSTRUCTION.** In
24 applying and construing this uniform act, consideration must be given to the need to promote
25 uniformity of the law with respect to its subject matter among states that enact it.

SECTION 11. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT.

1 Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001 *et seq.*, but does not
2 modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize
3 electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C.
4 Section 7003(b).

5 **[SECTION 12. SEVERABILITY.]** If any provision of this [act] or its application to
6 any person or circumstance is held invalid, the invalidity does not affect other provisions or
7 applications of this [act] which can be given effect without the invalid provision or application,
8 and to this end the provisions of this [act] are severable.]

9 *Legislative Note:* Include this section only if this state lacks a general severability statute or a
10 decision by the highest court of this state stating a general rule of severability.

11 **SECTION 13. APPLICABILITY.** This [act] applies to:

13 (1) each will executed on or after the effective date of this [act]; and
14 (2) each proceeding pending in court or commenced after the effective date of this [act],
15 unless the court determines that it is not feasible to apply the [act] or, in the interests of justice,
16 the [act] should not apply.

17 **SECTION 14. REPEALS; CONFORMING AMENDMENTS.**

18 (a) ...
19 (b) ...
20 (c) ...

21 **SECTION 15. EFFECTIVE DATE.** This [act] takes effect....