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.
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
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>SECTION</th>
<th>TITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SHORT TITLE</td>
</tr>
<tr>
<td>2</td>
<td>DEFINITIONS</td>
</tr>
<tr>
<td>3</td>
<td>SCOPE</td>
</tr>
<tr>
<td>4</td>
<td>AUTHORITY OVER DIGITAL ASSETS AND COMMUNICATIONS OF DECEDENT BY PERSONAL REPRESENTATIVE</td>
</tr>
<tr>
<td>5</td>
<td>AUTHORITY OVER DIGITAL ASSETS AND ELECTRONIC COMMUNICATIONS OF PROTECTED PERSON BY [CONSERVATOR]</td>
</tr>
<tr>
<td>6</td>
<td>CONTROL OF DIGITAL ASSETS AND ELECTRONIC COMMUNICATIONS BY AGENT UNDER POWER OF ATTORNEY</td>
</tr>
<tr>
<td>7</td>
<td>CONTROL OF DIGITAL ASSETS AND ELECTRONIC COMMUNICATIONS BY TRUSTEE</td>
</tr>
<tr>
<td>8</td>
<td>FIDUCIARY AUTHORITY</td>
</tr>
<tr>
<td>9</td>
<td>COMPLIANCE</td>
</tr>
<tr>
<td>10</td>
<td>CUSTODIAN IMMUNITY</td>
</tr>
<tr>
<td>11</td>
<td>UNIFORMITY OF APPLICATION AND CONSTRUCTION</td>
</tr>
<tr>
<td>12</td>
<td>RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT</td>
</tr>
<tr>
<td>13</td>
<td>SEVERABILITY</td>
</tr>
<tr>
<td>14</td>
<td>APPLICABILITY</td>
</tr>
<tr>
<td>15</td>
<td>REPEALS; CONFORMING AMENDMENTS</td>
</tr>
<tr>
<td>16</td>
<td>EFFECTIVE DATE</td>
</tr>
</tbody>
</table>
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.

---


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.
SECTION 1. SHORT TITLE. This [act] may be cited as the Fiduciary Access to Digital Assets Act.

SECTION 2. DEFINITIONS. In this [act]:

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

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

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

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

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

(6) “Custodian” means a person that stores, or has control of, digital assets or electronic communications of an account holder.

(7) “Digital asset” means: a) information created, generated, sent, communicated, received, or stored by electronic means on a digital device or system that delivers digital information, and includes a contract right; and b) an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information which the account holder is entitled to access.

(8) “Digital device” means an electronic device that can receive, store, process, or send digital information.
(9) “Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(10) “Electronic communication” means a transfer of a sign, signal, writing, image, sound, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system. The term does not include a wire or oral communication; any communication made through a tone-only paging device; or any communication from a tracking device.

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

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

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

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

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

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

(17) “Power of attorney” means a record that grants an agent authority to act in the place of a principal.
(18) “Principal” means an individual who grants authority to an agent in a power of attorney.

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

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

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

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

(23) “Will” means a testamentary instrument. The term includes a codicil and a 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 assets created through employment generally belong to the employer. A custodian includes an electronic service provider as well as any other entity that provides or stores electronic data.
The definition of “electronic communication” excludes a variety of communications to ensure that they are treated as digital assets rather than electronic communications, a distinction that is significant in later sections of the act.

SECTION 3. SCOPE. This [act] applies only to a grant of authority to a fiduciary.

Comment

This section distinguishes the authority of fiduciaries, who exercise authority subject to this act only on behalf of the account holder from any other efforts to access the digital assets and electronic communications. Family members or friends may seek such access, but, unless they are fiduciaries, their efforts are subject to other laws and are not covered by this act.

SECTION 4. AUTHORITY OVER DIGITAL ASSETS AND COMMUNICATIONS OF DECEDENT BY PERSONAL REPRESENTATIVE.

(a) Unless prohibited by the will of the decedent, a court, or law of this state other than this [act], a personal representative of the decedent may obtain:

(1) the digital assets of a decedent;

(2) records of the electronic communications of the decedent controlled by an electronic communication service or a remote computing service, including a log of the electronic address of each party with whom the decedent communicated; and

(3) the contents of each electronic communication controlled by an electronic communication service or a remote computing service sent or received by the decedent, to the extent consistent with 18 U.S.C. Section 2702(b).

(b) Once obtained, a personal representative may access, manage, deactivate, and delete the digital assets and the records and contents of the electronic communications of a decedent.

Comments for the Committee

Subsection (a)(1) establishes the default rule that the personal representative is authorized to administer all of the decedent’s digital assets other than material covered by the Electronic Communications Privacy Act (ECPA). It is modeled on the formulation of the personal representative’s default power set out in UPC Sec. 3-715.

The subsection clarifies the difference between fiduciary authority over digital assets
other than electronic communications protected by ECPA, and authority over ECPA-covered
electronic communications. For electronic communications, subsections (a)(2) and (3) establish
procedures that cover: first, logs and records that providers may release without consent under
ECPA; and second, ECPA-covered communications. Federal law distinguishes between the
permissible disclosure of the “contents” of a communication, covered in 18 U.S.C. § 2702(b),
and of “a record or other information pertaining to a” subscriber or customer, covered in
18 U.S.C. § 2702(c). The first, content-based material, can be divided into two types of
communications: those received by the account holder and those sent. Material when the
account holder is the “addressee or intended recipient” can be disclosed either to that individual
or to an agent for that person. 18 U.S.C. § 2702(b)(1). Material for which the account holder is
the “originator” (as well as an addressee or intended recipient) can be disclosed with the account
holder’s “lawful consent.” 18 U.S.C. § 2702(b)(3). (Note that, when the account holder is the
addressee or intended recipient, material can be disclosed under either (b)(1) or (b)(3), but that
when the account holder is the originator, lawful consent is required. By contrast to content-
Based material, non-content material can be disclosed not only with the lawful consent of the
account holder but also to any person other than a governmental entity (which would presumably
include fiduciaries). (Further discussion of this issue is set out in the Comments to Section 8,
infra.)

Several people have raised the issue of whether this authority must be specifically
granted in a court order or whether it should be a default power. That’s an issue for Committee
discussion. The Committee might want to revisit issues involving dead hand control in the face
of language in a will that prohibits access to any digital assets.

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.

SECTION 5. AUTHORITY OVER DIGITAL ASSETS AND ELECTRONIC
COMMUNICATIONS OF PROTECTED PERSON BY [CONSERVATOR].

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

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

(c) At a hearing concerning the appointment or authority of a [conservator] for an
individual or a protected person, a court may authorize a [conservator] to obtain:

(1) the digital assets of an individual or a protected person;
(2) records of the electronic communications of an individual or a protected
person controlled by an electronic communication service or a remote computing service,
including a log of the electronic address of each person with whom the individual or protected
person communicated; and

(3) the contents of each electronic communication controlled by an electronic
communication service or a remote computing service sent or received by the individual or
protected person to the extent consistent with 18 U.S.C. Section 2702(b).

(4) Once obtained, the [conservator] may access, manage, deactivate, and delete
the digital assets and the records and contents of electronic communications of the individual or
protected person.

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

**Comments for the Committee**

Section 5 establishes that the conservator must be specifically authorized by the court to
access the protected person’s digital assets. Each of the different levels of access must be
specifically granted by court order. The Committee may need to clarify that the requirement in
Section 5 for express authority over digital assets does not limit the fiduciary’s authority over
the underlying “bricks and mortar” assets, such as a bank account.

Section 5 is comparable to Section 4. It responds to the concerns of internet service
providers who believe that the act should be structured to clarify the difference between fiduciary
authority over digital assets other than electronic communications protected by federal law, the
Electronic Communications Privacy Act (ECPA), and authority over ECPA-protected electronic
communications. Consequently, this draft sets out procedures that cover: first, logs and records
that providers may release without consent under ECPA; and second, ECPA-covered
communications.

Subsection (c) is comparable to Section 4(a) with respect to the separation of authority
over digital assets and electronic communication subject to ECPA.

Subsection (d) repeats the introductory language in UPC Section 5-411(c), and is
designed to clarify that a decision by the court to grant powers to the conservator under this
section must be based primarily on the decision that the protected person would have made, if of full capacity. The protected person’s personal values and expressed desires, past and present, are to be considered when making decisions about the conservator’s authority. Existing state law may also set out the requisite standards for a conservator’s actions, and the bracketed language allows for reference to those laws. Under Section 8, the conservator has the same power over digital assets as the account holder. The conservator must exercise authority in the interests of the protected person.

SECTION 6. CONTROL OF DIGITAL ASSETS AND ELECTRONIC COMMUNICATIONS BY AGENT UNDER POWER OF ATTORNEY. If a power of attorney grants authority to an agent over digital assets and electronic communications of a principal, and exercise of the authority is not otherwise prohibited by a governing instrument, the agent may:

(1) access, manage, deactivate, and delete the digital assets and electronic communications; and

(2) change a governing instrument, other than the power of attorney, affecting the digital assets and electronic communications.

Comments for the Committee

This section establishes that the agent must be specifically authorized by the principal to access the principal’s digital assets and electronic communications, and it is modeled on UPC Sec. 5B-201(a). Because a power of attorney contains the consent of the account holder, ECPA should not prevent the agent from exercising authority over the content of electronic communications. There should be no question that an explicit delegation of authority in a power of attorney constitutes authorization from the account holder to access digital assets, and provides “lawful consent” to allow disclosure of electronic communications from an electronic communication service or a remote computing service pursuant to applicable law. Both authorization and lawful consent are important because 18 U.S.C. § 2701 deals with intentional access without authorization and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

The American College of Trusts and Estates Counsel’s State Laws Committee recently asked the Committee to consider whether the authority over digital assets and electronic communications, instead. The Committee has decided this power must be expressly granted, because when expressed and not default, it satisfies the lawful consent requirement of ECPA.

An issue for the Committee is how the agent accesses the digital assets. Is access in the name of the agent or the principal? Outside of the digital world, it is clear that the agent is not the
principal. But is this an issue we even need to address?

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

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

SECTION 7. CONTROL OF DIGITAL ASSETS AND ELECTRONIC COMMUNICATIONS BY TRUSTEE. A trustee may access, manage, deactivate, and delete the digital assets and electronic communications held in the trust in accordance with the terms of the trust expressly authorizing the trustee to exercise these powers.

Comments for the Committee

A trustee may have title to digital assets and electronic communications both through an account created by and used by the principal and an account created by the fiduciary for fiduciary business. There should be no question that holding property in trust form constitutes authorization from the account holder to access digital assets, and that it provides “lawful consent” to allow disclosure of electronic communications from an electronic communication service or a remote computing service pursuant to applicable law. Both authorization and lawful consent are important because 18 U.S.C. § 2701 deals with intentional access without authorization, and 18 U.S.C. § 2702 allows a provider to disclose with lawful consent.

SECTION 8. FIDUCIARY AUTHORITY.

(a) A fiduciary with authority over digital assets or electronic communications of an account holder under this act:

(i) has the same authority as the account holder;

(ii) has the lawful consent of the account holder; and

(iii) is an authorized user of the account.

(b) The rights of the fiduciary exercising the account holder’s authority are subject to copyright and other law as well as any applicable and enforceable terms of service agreement.
(c) The exercise of authority over digital assets or electronic communications by a fiduciary is not a transfer of property, notwithstanding a contrary provision in a terms of service agreement.

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

Comment

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

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

The Stored Communications Act contains two potentially relevant prohibitions.

1) 18 U.S.C. § 2701(a), which concerns access to the digital assets, makes it a crime for anyone to “intentionally access [] without authorization a facility through which an electronic communication service is provided” as well as to “intentionally exceed [] an authorization to

---


access that facility.” Thus, someone who has authorization to access the facility is not engaging in criminal behavior. Moreover, this section does not apply to “conduct authorized . . . by a user of that service with respect to a communication of or intended for that user.”

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

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

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

Subsection (b) similarly reinforces the concept that the fiduciary “steps into the shoes” of the account holder, with no more – and no fewer – rights. For example, the terms of service agreement controls the rights of the account holder (settlor, principal, incapacitated person, decedent). The Act does not permit the account holder’s fiduciary to override the TOSA in order to make a digital asset or collection of digital assets “descendible,” although it does preserve the rights of the fiduciary to make the same claims as the account holder. See Ajemian v. Yahoo!, Inc., 987 N.E.2d 604 (Mass. 2013); David Horton, Indescendibility, 102 Calif. L. Rev. __ (forthcoming 2014), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2311506.

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

---

7 18 U.S.C. §§ 2701(a), (c)(2).
SECTION 9. COMPLIANCE.

(a) If the fiduciary of an account holder complies with subsection (b) and makes a request in a record to a custodian of digital assets or electronic communications of the account holder for access to the assets and communications or ownership or a copy of the assets or communications, the custodian must comply with the request.

(b) If a request under subsection (a) is made by:

(1) a personal representative with authority under Section 4 the request must be accompanied by a certified copy of the letter of appointment of the representative;

(2) a [conservator][ with authority under Section 5], the request must be accompanied by a certified copy of the court order that gives the [conservator] authority over the digital assets or electronic communications;

(3) an agent [with authority under Section 6], the request must be accompanied by a certified copy of the power of attorney that authorizes the agent to exercise authority over the digital assets or electronic communications; and must be accompanied by an affidavit in which the affiant attests that the record is an accurate record of the original of the power and that, to the best of the affiant’s knowledge, the power remains in effect; or

(4) a trustee [with authority under Section 7], the request must be accompanied by a certified copy of the trust instrument or a certification of the trust under [cite trust certification statute, such as Uniform Trust Code Section 1013] that authorizes the trustee to exercise authority over the digital assets or electronic communications.

(c) A custodian shall comply with a request made under subsection (a) not later than [60] days after receipt of the request. If the custodian fails to comply, the fiduciary may apply to the court for an order directing compliance.
[(d) Instead of furnishing a copy of a trust instrument under subsection (c)(4), the trustee may furnish a certification of trust. A certification of trust:

(1) must contain the following information:

(A) that the trust exists and the date the trust instrument was executed;
(B) the identity of the settlor;
(C) the identity and address of the currently acting trustee;
(D) the powers of the trustee;
(E) the revocability or irrevocability of the trust and the identity of any person holding a power to revoke the trust;
(F) the authority of a co-trustee to sign or otherwise authenticate, and whether all or less than all co-trustees are required to exercise powers of the trustee;
(G) the trust’s taxpayer identification number; and
(H) the manner of taking title to trust property;

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

(3) must state that the trust has not been revoked, modified or amended in a manner that would cause the representations contained in the certification of trust to be incorrect;

and

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

(f) A recipient of a certification of trust under subsection (e) may require the trustee to furnish copies of excerpts from the original trust instrument and later amendments which designate the trustee and confer on the trustee the power to act in the pending transaction.

(g) A custodian that acts in reliance on a certification under subsection (e) without knowledge that the representations contained in it are incorrect is not liable to any person for so
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.

(i) A person that demands the trust instrument in addition to a certification of trust under subsection (e) or excerpts under subsection (f) is liable for damages if the court determines that 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

The bracketed material allows states that have already enacted the UTC to use the shorter version. Those states that have not adopted the UTC may choose to include the bracketed 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.

SECTION 10. CUSTODIAN IMMUNITY. A custodian and its officers, employees, 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.

SECTION 11. UNIFORMITY OF APPLICATION AND CONSTRUCTION. In applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

SECTION 12. RELATION TO ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT. This [act] modifies, limits, or supersedes the Electronic
Signatures in Global and National Commerce Act, 15 U.S.C. Section 7001 et seq., but does not modify, limit, or supersede Section 101(c) of that act, 15 U.S.C. Section 7001(c), or authorize electronic delivery of any of the notices described in Section 103(b) of that act, 15 U.S.C. Section 7003(b).

[SECTION 13. SEVERABILITY. If any provision of this [act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [act] which can be given effect without the invalid provision or application, and to this end the provisions of this [act] are severable.]

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

SECTION 14. APPLICABILITY. This [act] applies to:

(1) each will executed on or after the effective date of this [act]; and

(2) each proceeding pending in court or commenced after the effective date of this [act], unless the court determines that it is not feasible to apply the [act] or, in the interests of justice, the [act] should not apply.

SECTION 15. REPEALS; CONFORMING AMENDMENTS.

(a) …

(b) …

(c) …

SECTION 16. EFFECTIVE DATE. This [act] takes effect....