Published by the Estate Planning and Administration Section of the Oregon State Bar

Newsletter

Oregon Estate Planning and Administration Section Newsletter
Volume XXXIII, No. 4
December 2016

Oregon State Bar Estate Planning & Administration Section

Oregon's New Uniform Digital Assets Law: Estate Planning and Administration in the Information Age

Michael D. Walker
Samuels Yoelin Kantor LLP
Portland, Oregon

I. INTRODUCTION

Not so long ago, in a world not so far away, estate planning and the administration of a decedent's estate was typically a process that focused on the individual's tangible belongings, financial assets, and real estate. Aside from the federal tax laws, state statutes and common law primarily controlled all aspects of the planning and administration of a decedent's estate. However, in the Information Age where almost every aspect of our lives is in some manner affected or controlled by information that is stored in an electronic form, it is not surprising that the impact of "digital assets" has fundamentally and irrevocably changed the nature of the estate planning and administration practice.

Starting in the 1980s with the passage of the Stored Communications Act ("SCA")[1] and the Computer Fraud and Abuse Act ("CFAA"),[2] Congress has enacted federal statutes that have a profound effect on the legal status of digital assets. However, these statutes generally do not address the impact of the death or incapacity of the owner or creator of those digital assets. In the last several years, the efforts of the Uniform Law Commission ("ULC") have culminated in the uniform statute known as the Revised Uniform Fiduciary Access to Digital Assets Act ("RUFADAA").[3] As of this writing, RUFADAA has now been passed by 21 states, including Oregon[4] and Washington.[5] In addition, all states have statutes that criminalize unauthorized access, or "hacking," of computer systems and networks.[6]

With such a mélange of state and federal laws, preparing effective estate planning documents for individuals, or administering the estates of incapacitated persons and decedents, presents a unique and difficult set of challenges. In approaching these challenges, the practitioner will be benefitted by having a working understanding of not only the elements of state law that impact digital assets, but also of the SCA and CFAA, particularly as those statutes are interpreted by the Internet and technology industry.

1 18 USC §§ 2701-2712 (2012).
2 18 USC § 1030 (2012).
3 Nat'l Conference of Comm'rs on Unif. State Laws, Revised Fiduciary Access to Digital Assets Act (2015), http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets%20Act,%20Revised%20 (hereinafter RUFADAA).
4 *See* Or Laws 2016, ch 19. The effective date of the Oregon statute is January 1, 2017.
5 RCW § 11.120 (2016); 2016 Wash Sess Laws ch 140. The effective date of the Washington statute was June 9, 2016.
6 *See, e.g.,* ORS § 164.377; RCW § 9A.52.110, §§ 9A.52.120-130 (repealed), § 9A.48.100; SB 2375, 2016 Leg (Wash 2016); Cal Penal Code § 502 (2016).

In This Issue

II. WHAT ARE DIGITAL ASSETS?

My favorite professor in college frequently admonished his students that the key foundational element to any cogent analysis was to carefully define the relevant terms of that analysis. Hence, as a starting point, the somewhat illusive and amorphous term "digital assets" should be thoughtfully discussed.

a. RUFADAA Definition of Digital Assets.

RUFADAA states that a "digital asset" means an "electronic record in which an individual has a right or interest," but does not include the "underlying asset or liability unless the asset or liability is itself an electronic record."[7] In turn, a "record" is defined as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[8] Finally, "electronic" means "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities."[9]

As an initial observation, the definition of digital assets refers to an electronic record that is owned by an "individual." Hence, this definition would appear to exclude any digital asset that is owned by an estate or business entity, all of which *are* included within RUFADAA's separate definition of "person."[10] The ULC's comments do not address this nuance, and the consequences of this language are unclear.

The definition of "digital asset" includes any type of electronically-stored information, including electronic information stored on a user's computer or any other digital device, content uploaded to the Internet, and rights in digital property.[11] It also includes records that are either the catalogue or the content of an electronic communication.[12]

b. Practical Scope of Digital Assets Definition.

Digital assets include any electronically-stored information, regardless of whether the location of that storage is the Internet (including social media applications and email services), a private computer network, a personal computer, a tablet, a memory drive, or a mobile phone. The definition's proviso, "*unless the asset or liability is itself an electronic record*," also has important consequences. For example, digital currency such as bitcoin would be an asset that is itself an electronic record. An Internet domain name would also be considered an asset that is also an electronic record. Finally, commercial loyalty points and awards, such as accrued airline miles and hotel points, would be considered digital assets, although many are subject to contractual restrictions and cannot be transferred to the heirs of a deceased customer.[13] However, as discussed below, online digital assets are typically subject to a term of service agreement ("TOSA"), even following the death or incapacity of the owner of the digital asset.

c. Economic and Non-Economic Value of Digital Assets.

In a 2011 McAfee survey, American households valued their digital assets at nearly $55,000.[14] Certainly, many digital assets, such as bitcoin, commercial domain names, and similar property, have an ascertainable value that must be included as part of the administration of the estate of an incapacitated individual or a decedent's estate. For an estate subject to federal and/or state estate taxes, the value of such property will need to be determined and included on the pertinent estate tax returns. Likewise, such property may need to be separately listed on any required inventories of a decedent's estate.[15]

Many other forms of digital assets have no extrinsic economic value, but may have tremendous sentimental value. For example, most photographs are now created by digital cameras and stored in some digital form, often within a user's account with an online provider such as Facebook, Instagram, Flickr, and Photobucket. However, once uploaded to these sites, these important family photos are subject to each provider's TOSA, which in turn may limit the access to such accounts to the user's fiduciaries upon incapacity or death.

III. FEDERAL LAW AFFECTING DIGITAL ASSETS

a. Stored Communications Act.

Congress passed the SCA in 1986 as part of the Electronic Communication Privacy Act ("ECPA").[16] Drafted early in the era of electronic communications, Congress sought to deal with the impact of Internet communications upon Fourth

7 RUFADAA, *supra* note 3, at § 2(10). The Oregon version of RUFADAA (Or Laws 2016, ch 19 (2016)) has not yet been codified under Oregon Revised Statutes. A conversation with the Oregon Legislative Counsel's office indicates that such codification is not expected until after the 2017 general session of the Oregon Legislature. Oregon's RUFADAA sections under Oregon Laws, chapter 19 (2016), generally follow the section numbers of the ULC's version of RUFADAA, with only stylistic differences in subsection references. Hence, subsequent citations will use the section numbers of the ULC version of the act.

8 *Id.* at § 2(22).

9 *Id.* at § 2(11).

10 *Id.* at § 2(17).

11 *Id.* at § 2 cmt.

12 *Id.*

13 *See, e.g.,* Kara Brandeisky, *What Happens to Your Airline Miles When You Die?* Time, July 31, 2015, http://time.com/money/3978458/airline-miles-death/.

14 Intel Security Group, *McAfee Reveals Average Internet User Has More Than $37,000 in Underprotected "Digital Assets,"* http://www.mcafee.com/us/about/news/2011/q3/20110927-01.aspx (last visited Dec. 7, 2016).

15 *See, e.g.,* ORS § 113.165 (2015).

16 SCA, 18 U.S.C. §§ 2701-2712 (2012).

Amendment privacy protections. The SCA states that a provider of either an "electronic communication service" or "remote computing service" may not "knowingly divulge to any person or entity the contents of a communication which is carried or maintained on that service." [17]

However, the SCA contains several key exceptions. First, the SCA does not prevent providers from providing non-governmental entities with a user's *non-content* information, such as the name of the person connected with the account in question.[18] An appropriate analogy to understand non-content information is to contrast the "envelope" containing a letter as containing non-content information, with the letter inside that envelope containing the "content" of the communication. Second, the statute allows the disclosure of content-based information to an "agent" of the addressee or intended recipient of an electronic communication.[19] Third, and most notably, a provider "may" disclose content information with the "*lawful consent* of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of a remote computing service."[20]

What is "lawful consent" in the context of digital assets owned by a decedent's estate or incapacitated person? While personal representatives and executors generally have the statutory authority under state law to take all necessary actions to administer the decedent's estate, this state-law authority does not automatically equate to the authority to grant "lawful consent" to the disclosure of the content of digital assets under the SCA.

The only federal court that had the opportunity to address this question declined to rule on the issue. In 2008, Sahar Daftary ("Sahar"), an internationally-known model, died following a fall from her twelfth floor building in England. In the inquiry that followed, Sahar's executors sought access to her Facebook account, which they believed contained critical evidence of Sahar's state of mind at the time of her death. In the ex parte proceeding that followed, the executors sought a subpoena in federal court in California. Facebook responded, and requested the court quash the subpoena, arguing that the subpoena violated the SCA. The court agreed, and in declining to decide whether Sahar's executors could provide the sufficient "lawful consent" under the SCA, the court stated that it

> lacks jurisdiction to address whether the Applicants may offer consent on Sahar's behalf so that Facebook may disclose the records voluntarily. Any such ruling would amount to nothing less than an impermissible advisory opinion. Of course, nothing prevents Facebook from concluding on its own that Applicants have standing to consent on Sahar's behalf and providing the requested materials voluntarily.[21]

Even if the court had explicitly found that the executor's fiduciary authority was sufficient to constitute "lawful consent" under the SCA, the language of the pertinent provisions of the SCA's exceptions states that the provider "*may* divulge the contents of a communication."[22] Given the discretionary language of the statute, and the absence of clear authority, the reality is that providers are reluctant to risk litigation and liability exposure in making a potentially incorrect decision and therefore will be hesitant to disclose a decedent's digital assets to a personal representative solely based upon the authority to do so under the SCA.

b. Computer Fraud and Abuse Act (and Similar State Statutes).

Congress passed the CFAA in 1986.[23] In relevant part, the CFAA imposes both criminal and civil liability upon anyone who "intentionally accesses a computer without authorization or exceeds authorized access," and obtains information from any "protected computer."[24] In addition, all 50 states have statutes that criminalize "unauthorized access" or "hacking" of computers and computer systems.[25]

In analyzing whether a fiduciary possesses legal authority for purposes of the CFAA and state counterparts, at least two essential issues should be analyzed. First, under either the governing instruments and/or relevant state law, does the fiduciary have clear legal authority to access the computer or digital assets of the decedent or incapacitated individual? Second, if the computer system or digital asset is subject to the terms and conditions of a TOSA, does the fiduciary's access violate the terms of that TOSA? Hence, a fiduciary with ostensible legal authority may still violate the CFAA if the fiduciary's access clearly violates the terms of the TOSA. For example, the U.S. Justice Department has

17 *Id.* at § 2702(a)(1)-(2).

18 *Id.* at § 2702(a)(3).

19 *Id.* at § 2702(b)(1).

20 *Id.* at § 2702(b)(3) (emphasis added).

21 *In re Facebook, Inc.*, 923 F Supp 2d 1204, 1206 (ND Cal 2012).

22 18 USC § 2702(b) (emphasis added).

23 Computer Fraud and Abuse Act, Pub L No. 99-474, 100 Stat 1213 (codified at 18 USC § 1030 (2012)).

24 18 USC § 1030(a)(2)(C). For purposes of the CFAA, a "protected computer" is defined at 18 USC § 1030(e)(2) as a computer exclusively for the use or affecting the "use of a financial institution or the United States Government," or "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

25 *See* Nat'l Conference of State Legis., *Computer Crime Statutes* (May 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

used the CFAA to prosecute individuals based *solely* upon the violation of the terms of a TOSA.[26]

IV. THE REVISED FIDUCIARY ACCESS TO DIGITAL ASSETS ACT: THE DIGITAL ASSETS "MULLIGAN"

a. Original UFADAA.

The ULC approved the "original" Uniform Fiduciary Access to Digital Assets Act ("UFADAA") in 2014.[27] Thereafter, UFADAA was introduced in approximately 27 states,[28] including Oregon.[29] A key component of the original UFADAA was that, subject to the SCA as well as any applicable TOSA, fiduciaries were legally imputed with lawful authority to administer the digital assets of a decedent or protected person in the same manner as provided under state law with respect to other, non-digital, assets.[30] UFADAA went as far as stating that a fiduciary had "under applicable electronic privacy laws, the *lawful consent* of the account holder for the custodian to divulge the content of an electronic communication to the fiduciary."[31]

However, the proposed legislation was met with strenuous opposition from lobbyists for the online providers. The providers raised a number of arguments. First, contrary to UFADAA's presumptive access stance, the providers argued that the default position of a decedent or incapacitated person was that their digital assets should *not* be disclosed to anyone, even to their fiduciary. Second, the providers took the position that UFADAA could not create a legal presumption of "lawful consent" for purposes of the SCA, and that UFADAA was preempted by federal law. Third, the providers argued that UFADAA should not override or supersede their TOSAs in any way.[32] Lastly, there were indications that the providers were concerned about civil litigation liability exposure and the cost of complying with UFADAA. As a result of these lobbying efforts, UFADAA passed only in Delaware, which had passed a version of UFADAA from a draft 2014 version.[33]

b. RUFADAA Compromise.

Following the near-complete failure of UFADAA, representatives from the ULC and the digital provider industry entered into a series of negotiations to discuss a compromise, the result of which was RUFADAA. The ULC formally approved the final draft of RUFADAA in July 2015.[34] Unlike the Original UFADAA, which granted fiduciaries *presumptive* authority to access digital assets, RUFADAA places great emphasis upon whether the deceased or incapacitated user *expressly* consented to the disclosure of the content of the digital assets, through either what RUFADAA refers to as an "online tool" or an express grant of authority in the user's estate planning documents or power of attorney. Hence, RUFADAA respects the concept of "lawful consent" under the SCA, and, unlike UFADAA, does not attempt to impute such lawful consent to the fiduciary. RUFADAA was adopted in Oregon in 2016 and the effective date of the Oregon statute is January 1, 2017.

c. Explanation of RUFADAA Provisions.

The following is a section-by-section summary of RUFADAA's provisions, using the section numbers from the uniform act.

Section 2 of RUFADAA sets forth a list of definitions used in the Act. While a comprehensive discussion of each definition is beyond the scope of this article, several of the key definitions are discussed below. Many of RUFADAA's definitions are based on those in the Uniform Probate Code.[35]

A "*custodian*" is defined as "a person that carries, maintains, processes, receives, or stores a digital asset of a user."[36] Hence, a custodian will include most providers of online email and social media services.

The term "*content of an electronic communication*" is adapted from the SCA, which provides that content, "when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication."[37] The definition is designed to cover only content subject to the coverage of the ECPA (including the SCA).[38] Consequently, the "content of an electronic communication," as used later throughout the revised UFADAA, refers only to information in the body of an electronic message that is

26 Sasha A. Klein & Mark R. Parthemer, *Who Will Delete the Digital You? Understanding Fiduciary Access to Digital Assets*, Probate and Property Magazine, July-Aug. 2016, at 3, http://www.americanbar.org/publications/probate_property_magazine_2012/2016/july_august_2016/2016_aba_rpte_pp_v30_4_article_klein_parthemer_understanding_fiduciary_access_to_digital_assets.html.

27 Nat'l Conference of Comm'rs on Unif. State Laws, Fiduciary Access to Digital Assets, http://www.uniformlawcommission.org/Committee.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets (last visited Dec. 7, 2016) [hereinafter "Original UFADAA"].

28 Kirkland, Robert K., *Pixar for Estate Planners: Who Gets Your Digital Stuff When You've Logged Off for the Final Time*, American Law Institute 27, Sept. 13, 2016.

29 SB 369 (2015).

30 *See, e.g.,* Original UFADAA, *supra* note 27, at §§ 3, 7.

31 *Id.* at § 7(a)(2) (emphasis added).

32 Klein & Parthemer, *supra* note 26, at 4.

33 *Id.*

34 RUFADAA, *supra* note 3, title page.

35 *Id.* at § 2 cmt; *id.* at § 2(10) (discussing the definition of "digital asset").

36 *Id.* at § 2(8).

37 18 USC § 2510(8).

38 RUFADAA, *supra* note 3, at § 2 cmt.

not readily accessible to the public. If the information were readily accessible to the public, it would not be subject to the privacy protections of federal law under the ECPA. For example, a "tweet" by a Twitter user that is accessible to the public at large would *not* fall under this definition.

In contrast, the definition of "*catalogue of electronic communications*" means information that identifies each person with which a user has had an electronic communication, the time and date of the communication, and the electronic address of the person.[39] For example, a catalogue relating to an email would be email addresses of the sender and the recipient, and the date and time the email was sent. Generally, a fiduciary will have access to a catalogue of the user's communications, but not the content, unless (as discussed below) the user consented to the disclosure of the content.[40]

RUFADAA defines an "*online tool*" as "an electronic service provided by a custodian that allows the user, in an agreement distinct from the terms-of-service agreement between the custodian and user, to provide directions for disclosure or nondisclosure of digital assets to a third person."[41] An online tool can provide for a "designated recipient" to administer the digital assets of the user.[42] As discussed below, an online tool will supersede directions in the user's estate planning documents, even if those directions are *contrary* to the user's preferences as expressed in an online tool.

Section 3 of RUFADAA provides that the act applies to (1) a fiduciary acting under a will or power of attorney signed before or after the effective date of the act, (2) a personal representative of a decedent who died before or after the effective date of the act (including a decedent who died intestate), (3) a conservatorship commenced before or after the effective date of the act, and (4) a trustee of a trust created before or after the effective date of the act.[43]

RUFADAA **Section 4** establishes a "three-tier priority system"[44] for determining a user's intent with respect to any digital asset. First, through an online tool, the user may direct the custodian whether to disclose the content of the digital asset. If the online tool allows the user to modify or delete the direction at any time, then any such direction "overrides a contrary direction by the user in a will, trust, power of attorney, or other record."[45] Second, if an online tool is not utilized, then the user's directions in a will, trust, power of attorney, or "other record" will control whether the content of a digital asset may be disclosed to a fiduciary.[46] Finally, if the user provides no direction in either an online tool or applicable documents, then the TOSA controlling the digital asset will govern the rights of the fiduciary.[47] If, as in most instances, the TOSA is silent as to the rights of a user's fiduciary, then RUFADAA's default rules (discussed below) will be the fiduciary's sole remaining option.

Section 5 of RUFADAA states that if a fiduciary obtains access to a digital asset, then the TOSA continues to apply to the fiduciary in the same manner as the original user. [48] A custodian is not required to permit a fiduciary to assume the rights under the TOSA if the custodian can comply with Section 6.[49]

Section 6 establishes the procedure by which a custodian may comply with RUFADAA's disclosure procedures. In particular, when disclosing a digital asset, the custodian, at its "*sole discretion*," may grant the fiduciary or designated recipient: (1) "full access to the user's account," (2) "partial access to the user's account sufficient to perform the tasks with which the fiduciary or designated recipient is charged," or (3) an electronic or paper copy of the digital asset.[50] This section allows the custodian to seek guidance from the court if the custodian feels a request from a fiduciary would impose an "undue burden" upon the custodian.[51]

Section 7 is the first of RUFADAA's provisions that delineate the procedures by which fiduciaries may seek access to information from online providers regarding the digital assets of a deceased or incapacitated user. This

39 *Id.* at § 2(4).
40 *Id.* at prefatory cmt.
41 *Id.* at § 2(16). Google's "Inactive Account Manager" is an example of an online tool, and can be accessed at https://support.google.com/accounts/answer/3036546?hl=en&ref_topic=2382809. Facebook also provides for "Memorized Accounts" for deceased users, which allows the account to continue to be viewed, but content cannot be added to the account once it is placed into the "memorialized" status. Facebook also allows the user to appoint a "Legacy Contact." Information on Facebook's tools can be accessed at https://www.facebook.com/help/1506822589577997/.
42 RUFADAA, *supra* note 3, at § 2(9).
43 *Id.* at § 3 & cmt.
44 *Id.* at § 4 cmt. Arguably, the act's judicial procedure, discussed below, could be viewed as a fourth tier, albeit not a preferable choice in most instances.
45 *Id.* at § 4(a).
46 *Id.* at § 4(b). At this tier, it is important to note that RUFADAA refers to "disclosure," and not "access." Those concepts are distinct under the statute.
47 *Id.* at § 4(c).
48 *Id.* at § 5.
49 *Id.* at § 5 cmt.
50 *Id.* at § 6(a).
51 *Id.* at § 6(d). This guidance may include an order from the court to disclose a subset limited by the date of the user's digital assets, all or none of the user's digital assets, or all of the user's digital assets to the court for review in camera.

section allows the personal representative of a decedent's estate to obtain such access if a court so directs or the personal representative gives the custodian: (1) a written request for disclosure in written or electronic form, (2) a certified copy of the user's death certificate, (3) a certified document evidencing the authority of the personal representative (such as court-issued letter of appointment or letters testamentary), and (4) unless the user utilized an online tool, a written document showing the user's "consent to disclosure of the content of electronic communications."[52]

In addition, Section 7 further provides that if the custodian requests, the personal representative can be required to provide the custodian with additional information, including evidence to show the user had an account with the custodian, which could include the account number, username, address, or other unique identifying information.[53] *In addition*, the custodian can also request that the fiduciary obtain a court order finding that: (1) the user had an account with the custodian, (2) disclosure of the content of the electronic communications does not violate the SCA, (3) unless the user utilized an online tool, that the user consented to the disclosure, *or* (4) disclosure of the information is "reasonably necessary for administration of the estate."[54]

The judicial procedures contemplated by Section 7 present serious challenges to the personal representative. The introductory phrase of Section 7 allows disclosure of the content of a digital asset if a "court directs."[55] However, prior to such disclosure, the custodian may request a finding from the court that the disclosure would not violate the SCA and federal privacy statutes (*e.g.*, 47 USC § 222), and/or that the "user consented to the disclosure."[56] This provision directly implicates the issue of whether, under federal law, a fiduciary appointed pursuant to state law has the user's "lawful consent" under the SCA to receive the content of an electronic communication. As seen in the *In re Facebook, Inc.* case discussed above,[57] courts appear to be reluctant to *imply* consent solely by the fact that the personal representative is serving in a fiduciary capacity. This dilemma thus places much greater importance upon a user granting express consent for disclosure of digital assets under the user's will, trust, and/or power of attorney.

Absent express consent in the decedent's will, **Section 8** of RUFADAA permits the personal representative to request that the custodian disclose a "catalogue of electronic communications sent or received by the user, *other than the content* of electronic communications of the user." [58] The procedure under Section 8 is similar to that described in Section 7, except that no copy of the decedent's will is required, and a finding by the court need not include references to compliance with the SCA because such non-content disclosures are not prohibited by the SCA. Hence, the fiduciary may still be able to receive non-content information from the custodian even if no basis for "lawful consent" under the SCA is present.

Under **Section 9** of RUFADAA, an agent under a power of attorney may request disclosure of content of a digital asset if the power of attorney "expressly grants" authority to the agent of such digital assets.[59] The request of the agent to the custodian must include: (1) a written request for disclosure in paper or electronic form, (2) an "original or copy of the power of attorney expressly granting the agent authority over the content of electronic communications of the principal," and (3) a certification by the agent, under penalty of perjury, that the power of attorney is in effect.[60] As in Section 7, the custodian may request that the agent provide identifier information or other evidence to confirm that the user has an account with the custodian.

Section 10 allows the agent under a power of attorney to seek a catalogue of electronic communications.[61] The agent must submit the request to the custodian, along with a copy of the power of attorney and certification under penalty of perjury that the power of attorney remains in effect.[62] As with Section 9, the custodian may request identifier information or other evidence to confirm an existing account.

Section 11 of RUFADAA states that, if a trustee is an "original user" of an account, then the trustee can access all digital assets of the account held in trust, together with a catalogue of all electronic communications.[63]

If the trustee of a trust is *not* the original user of an account but the account is transferred into a trust by the settlor or in another manner, then **Section 12** of RUFADAA sets forth a process by which the trustee may request disclosure of digital assets from the custodian. Unless ordered by the court, directed by the original user, or provided in the trust, a custodian shall disclose the digital

52 *Id.* at § 7(1)-(4).
53 *Id.* at § 7(5)(A)-(B).
54 *Id.* at § 7(5)(C).
55 *Id.* at § 7.
56 *Id.* at § 7(5)(C).
57 *See In re Facebook*, 923 F Supp 2d 1204; *see also Negro v. Superior Court of Santa Clara County*, 179 Cal Rptr 3d 215 (2014) (finding that state law can mandate disclosure of electronic communications, even if the SCA makes such disclosure discretionary when, in the facts of *Negro*, the user was found to have consented to such disclosure).
58 RUFADAA, *supra* note 3, at § 8 (emphasis added).
59 *Id.* at § 9. The "expressly consents" language makes it clear that a simple power of attorney, without explicit consent by the principal to permit disclosure of electronic communications to the agent, will likely not satisfy Section 9's requirement.
60 *Id.* at § 9(1)-(3).
61 *Id.* at § 10.
62 *Id.* at § 10(1)-(3).
63 *Id.* at § 11.

asset information to the trustee if the trustee gives the custodian: (1) a written request for disclosure in paper or electronic form, (2) a certified copy of the trust instrument or certification of trust[64] that includes consent to the disclosure of content of the digital asset to the trustee, and (3) a certification by the trustee, under penalty of perjury, that the trust exists and the trustee is a currently acting trustee of the trust. 65 The custodian may also request that the trustee provide identifier information and/or "evidence linking the account to the trust."[66]

RUFADAA's **Section 13** addresses the disclosure of non-content information (i.e., the catalogue of electronic communications). Under this section, the trustee is entitled to submit a request to the custodian by submitting a request similar to that described in Section 12, above, except that the copy of the trust instrument or certification of trust need not include a reference to consent to disclosure of the content of the digital asset. [67]

Section 14 of RUFADAA sets forth the process by which a conservator may receive limited information relating to the protected person's digital assets. This section is premised upon the notion that the protected person still retains privacy rights in his or her personal communications. [68] Hence, digital assets may only be accessed by an express order of the court, and not solely based on the conservator's general authority to manage the protected person's assets.[69] Except as may be otherwise directed by the court, the conservator may receive only the catalogue of the user's digital assets, and not content-based information.[70] Procedurally, the conservator is entitled to obtain this information by giving the custodian a request for such information in either paper or electronic format, along with a certified copy of the court's order.[71] In addition, a conservator with general authority over the protected person's digital assets may request that the custodian terminate or suspend the protected person's account for good cause.[72]

Section 15 of RUFADAA is an important section that specifies the nature and extent of a fiduciary's duties as they specifically relate to digital assets. Specifically, this section begins by confirming that the legal duties of a fiduciary that is "charged with managing tangible property" also apply to the management of digital assets.[73] These duties include (and are presumably not limited to) the duties of care, loyalty, and confidentiality.[74] In addition, Section 15 states that the fiduciary's authority over a digital asset: (1) is subject to any applicable TOSA, except as supplanted by the user's direction in an online tool or applicable documents expressing lawful consent (i.e., Section 4 of RUFADAA); (2) is subject to applicable law, including copyright law; (3) is limited by the scope of the fiduciary's duties; and (4) may not be used to "impersonate the user."[75]

If a digital asset is not held by a custodian or subject to a TOSA (e.g., digital files stored on a decedent's personal computer), then Section 15 confirms that the fiduciary has an unrestricted right to access such digital assets.[76] For purposes of state laws relating to computer fraud or unauthorized computer access,[77] a fiduciary acting within the scope of the fiduciary's duties is an authorized user of the property of a decedent, protected person, principal, or settlor.[78] Similarly, a fiduciary with authority over tangible personal property of a decedent, protected person, principal, or settlor, has the right to access such property and any digital asset stored thereon.[79] With respect to termination of a digital asset account, Section 15 states that: (1) a custodian may disclose to a fiduciary information in an account that is required in order to close such an account; and (2) a fiduciary may terminate the user's account by submitting a written request to the custodian, along with enumerated documentation to verify the fiduciary's authority and a death certificate, if the user in question is deceased.[80]

Section 16 of RUFADAA provides that, within 60 days after a custodian receives a request for disclosure from a fiduciary together with all information required by RUFADAA, the custodian shall comply with the request.[81] If the custodian fails to comply with the request, the fiduciary may seek a court order compelling compliance, but any such order must also contain a finding that "compliance is not in violation of 18 U.S.C. Section 2702." [82] Section 16 gives the custodian the authority to notify the original user of a disclosure request by a fiduciary.[83] Section 16 further provides that if the custodian is aware of "any lawful access to the account following the receipt of the fiduciary's

64 *See, e.g.,* Unif. Trust Code § 1013; *see also* ORS 130.860 (2015) (setting forth the requirements of a certification of trust).
65 RUFADAA, *supra* note 3, at § 12.
66 *Id.* at § 12(4).
67 *Id.* at § 13.
68 *Id.* at § 14 cmt.
69 *Id.* at § 14(a).
70 *Id.* at § 14(b).
71 *Id.*
72 *Id.* at § 14(c).
73 *Id.* at § 15(a).
74 *Id.*
75 *Id.* at § 15(b). "Impersonate" in this context is likely limited to actions by which the fiduciary "pretends" to be the user (for example, in a social media or email account). It is unlikely that a fiduciary that lawfully obtains access to a digital asset is "impersonating" the user for purposes of this section.
76 *Id.* at § 15(c).
77 *See, e.g.,* ORS 164.377 (2015).
78 RUFADAA, *supra* note 3, at § 15(d).
79 *Id.* at § 15(e).
80 *Id.* at §§ 15(f), (g).
81 *Id.* at § 16(a).
82 *Id.* at §§ 16(a), (b).
83 *Id.* at § 16(c).

request" under RUFADAA, then the custodian may deny that fiduciary's disclosure request.[84]

In addition, Section 16 does not limit a fiduciary's ability to obtain, *or* require a fiduciary to obtain, a court order that: (1) specifies the account belongs to a protected person or principal under a power of attorney, (2) finds there is "sufficient consent" from the protected person or principal to support the requested disclosure, or (3) contains a finding "required by law" other than RUFADAA.[85]

Finally, Section 16 states that a custodian (together with its officers, employees, and agents) is immune from liability for an "act or omission done in good faith in compliance" with RUFADAA.[86] The comments to RUFADAA further explain this section's grant of "immunity" indicates that the section shields custodians from "indirect" liability (e.g., if a custodian grants access under the act). However, this immunity would not apply to instances of "direct" liability, such as a custodian's noncompliance with a court order under RUFADAA.[87]

Sections 17 through 21 of RUFADAA contain several administrative provisions, including a uniformity provision.

V. ESTATE PLANNING IN CONJUNCTION WITH RUFADAA

a. Provide for "Lawful Consent" Under the SCA.

Under the current rubric of federal and state laws, including RUFADAA and its inherent deference to the "lawful consent" requirements of the SCA, the most important step in the entire process of planning is to include a clear expression of such "lawful consent" in the individual's applicable estate planning documents. These include the individual's will, general power of attorney, and any trust (including a revocable living trust) that may at any point interact with a digital asset. As seen above in the discussion of RUFADAA's disclosure procedures, absent a clear expression of a user's consent, the fiduciary will not be able to access the content within the digital asset, and may be limited to a "catalogue" of electronic communications.

While such catalogue information may in fact be helpful to the work of the personal representative in administering the estate, without corresponding content, such a catalogue could potentially raise more questions than answers. For the personal representative, this is the equivalent of reviewing the outside of an envelope without any ability to access the contents of that envelope.

Appendix A to these materials sets forth an illustrative provision to be adapted to an individual's will. However, with appropriate adjustments, this provision could be easily adapted to grant digital assets authority to a trustee of a trust, or an agent under a power of attorney. While there is certainly no "magic language" to be used in such a provision, there are several important elements to consider.

First, the individual should clearly express that they consent to the disclosure of the *content* of any digital asset to the fiduciary. This provision invokes the "lawful consent" provision of the SCA.[88] In order to provide a custodian with a high degree of "comfort" that the user intended the provision to be an "SCA consent," it is certainly helpful to cite the SCA and the CFAA directly in the provision. Second, the provision should give the fiduciary the authority to access a digital asset in any location, whether it is stored on a tangible digital device (such as a personal computer or memory drive) or at an Internet location. Third, the provision should give the fiduciary the authority to hire a "technical" expert or consultant to help the fiduciary access the content of a digital asset or possibly secure the integrity and security of an electronic device or online account. Lastly, the provision should clearly state that the fiduciary is an "authorized user" for purposes of applicable computer-fraud and unauthorized-computer-access laws, such as the CFAA.

b. Create a Virtual Assets Instruction Letter.

In 2011, the author and his law partner, Victoria Blachly, created the concept of a Virtual Asset Instruction Letter ("VAIL")." The VAIL is not a form, but an attempt to delineate an intentional process for dealing with a client's digital assets. Here are the steps of the VAIL process:

- Identify each digital asset and determine how the custodian of that asset treats the account of the user upon death or incapacity.
- Determine the digital assets that the fiduciary should maintain and/or have access to, and prepare a written or electronic list of those assets, together with their passwords.
- Determine the digital assets that the fiduciary should terminate, and provide the necessary instructions to do so.
- Consider saving the list of digital assets or instructions to a memory drive, then store that drive in a *very* secure location, such as a safe deposit box. Give your fiduciary instructions on how to access this list. Remember to update the list frequently to reflect new and updated passwords.
- Make sure that all relevant documents, including the will, trusts, powers of attorney, or other estate planning documents are updated to provide "lawful consent" under the SCA and RUFADAA.
- If someone other than your personal representative is designated to handle your digital assets, make sure

84 *Id.* at § 16(d).
85 *Id.*
86 *Id.* at § 16(f).
87 *Id.* at § 16 cmt.
88 18 U.S.C. § 2702(b)(3) (2012).

that such individuals are granted adequate authority and consent to access digital assets under state law, the SCA, and RUFADAA.

VI. FIDUCIARY ADMINISTRATION OF DIGITAL ASSETS

In an estate or trust administration, the fiduciary[89] should adhere to the common practices required by law in dealing with digital assets. These practices are now supplemented by the provisions of RUFADAA. However, while this area of the law is still developing, careful application of existing fiduciary standards will likely be helpful. This discussion would also be relevant in a similar context if a person loses mental capacity and a conservator or successor trustee is faced with similar dilemmas with respect to the incompetent person's assets.

a. Digital Assets and a Fiduciary's "Prudent Person" Standard.

In a general sense, a fiduciary's duty is often expressed as a "prudent person" standard. For example, Section 804 of the Uniform Trust Code states that a trustee "shall administer the trust as a prudent person would, by considering the purposes, terms, distributional requirements, and other circumstances of the trust."[90] However, how do these standards apply to a fiduciary's duties in dealing with digital assets held by an estate or a trust? First, comment "a" to Section 174 of Restatement (Second) of Trusts is helpful in stating that the standard of care and skill required of a trustee is an "external standard." Hence, the proliferation of digital assets in the modern world necessarily leads to the conclusion that a trustee's duties must evolve to meet the changing manner in which individuals own and manage their assets. In 1960, it would have been unlikely for a court to conclude that the "ordinary prudence" of a trustee would include a working knowledge of computer technologies. However, a court in the "information age" would likely reach a much different conclusion. The following discussion may provide the fiduciary with at least a starting point in evaluating the appropriate steps to meeting the "prudent" standard in the context of an estate or trust that owns a substantial number of digital assets.

b. Locating a Decedent's Digital Assets.

Consider the possibility of a decedent with substantial assets and a strong tendency to manage those assets electronically so as to leave only a limited "paper trail" in the traditional sense. If the decedent managed his or her assets online, received "paperless" account statements via email, maintained information about those assets on a "cloud" server, and generally communicated about those assets by email, unless the decedent undertook careful planning during his or her lifetime to grant proper "lawful consent" to his or her fiduciary, simply *finding* the decedent's digital assets may present a serious challenge.

If such a decedent had not planned adequately, what constitutes "prudent" action by the fiduciary may be difficult to ascertain. First, the fiduciary should consider whether it may be necessary to hire a forensic expert in information technologies to advise the fiduciary on a prudent process for locating a decedent's digital assets. After analyzing the applicable TOSAs, the fiduciary should attempt to determine whether it is possible to gain working access to important "portals" into the decedent's digital existence. This may include the decedent's personal computer(s), smartphone, or other digital storage devices. If the decedent utilized financial software (e.g., Quicken or Microsoft Money), entries found in such programs might lead to digital assets. Finally, sources such as tax returns and Forms 1099 could reflect assets that might not otherwise be found in traditional "paper records" such as account statements.

c. Administering an Estate with Digital Assets.

Presuming the decedent's digital assets can be located, there are a number of steps that the personal representative and/or trustee should consider.[91]

1. The fiduciary should use the procedures under RUFADAA to obtain disclosure of the digital assets from the relevant custodians.[92] A sample RUFADAA disclosure request letter is set forth in **Appendix B**. If the relevant documents (i.e., a decedent's will or the principal's power of attorney) contain sufficient consent under the SCA, the fiduciary should attempt to obtain the full access to the content of the

89 In this section, the use of the term "fiduciary" generally refers to any person charged with administering a decedent's estate or trust (i.e., an executor or personal representative of an estate, and a trustee of a trust). Most of the principles discussed in this section apply in the same manner to each type of fiduciary.

90 *See also* Restatement (Second) of Trusts § 174 (1959) (the trustee "is under a duty to the beneficiary in administering the trust to exercise such care and skill as a man of ordinary prudence would exercise in dealing with his own property . . ."); Unif. Prob. Code § 7-302 (the trustee "shall observe the standards in dealing with the trust assets that would be observed by a prudent man dealing with the property of another . . ."); ORS 130.665 (2015) (statute is identical to Section 804 of the Uniform Trust Code); Del Code tit 12, § 3302(a), Westlaw (database updated 2016) ("[A] fiduciary shall act with the care, skill, prudence and diligence under the circumstances then prevailing that a prudent person acting in a like capacity and familiar with such matters would use to attain the purposes of the account.").

91 *See also* Dennis Kennedy, *Estate Planning for Your Digital Assets*, Law Practice Today (Mar. 2010).

92 *See infra* Part IV.c.

relevant digital assets.[93] If such documents are silent as to the user's consent, the fiduciary should carefully review the relevant TOSAs in question and possibly request a "catalogue" of the digital assets under RUFADAA, as even the catalogue could potentially lead the fiduciary to the existence of unknown assets.

2. If the fiduciary obtains lawful access to digital assets,[94] the fiduciary should attempt to "marshal" such assets by making certain that the fiduciary is the only party that has access to the assets. For example, the fiduciary should consider changing the password that is used to access the asset. If the decedent had shared such a password with a family member or other individual who is not the fiduciary, then such a "digital interloper" could interfere with the fiduciary's ability to accomplish the proper administration of the estate or trust. The fiduciary should remove all private and/or personal data from online shopping accounts (or close them as soon as reasonably possible).
3. If the decedent had established any form of "automatic" means to pay bills, make loan payments, or deal with other debts, the fiduciary should determine the exact nature of these arrangements, then evaluate whether they should be continued, or (more likely) converted to a payment method that is consistent with the fiduciary's administrative and accounting procedures.
4. If possible, the fiduciary should endeavor to remove personal or sensitive data (such as credit card information) from online sites. This is yet another means to try to prevent identity theft or other unforeseen consequences.
5. While undertaking such control, the fiduciary should also take steps to archive important electronic data for the full duration of the relevant statutes of limitation. In this way, if data is updated during the course of administration, the fiduciary will have a "baseline" of data if beneficiaries or other parties raise questions or complaints in the future.
6. Along with all other assets under the fiduciary's control, the fiduciary should prepare a written inventory of the decedent's digital assets. If a digital asset has its own extrinsic value (such as a commercial website or online publication), then the value of such asset should be separately listed on the estate's or trust's asset inventory. While placing a value on such assets may be difficult, it is certainly not beyond the professional expertise of a qualified valuation professional. This step may also be relevant to the extent that the estate may be subject to federal estate tax or state-level transfer taxes.
7. The fiduciary should consider consolidating digital assets to as few "platforms" as possible (e.g., have multiple email accounts set to forward to a single email account). This may ease the fiduciary's administrative burden.
8. If appropriate, the fiduciary should consider notifying the individuals in the decedent's email contact list and other social media contacts. As these contacts may be very sensitive and personal in nature, the fiduciary may wish to consult with any appropriate family members before undertaking such communications.
9. The fiduciary should keep all accounts open for at least a period of time to make sure all relevant or valuable information has been saved and all vendors or other business contacts have been appropriately notified, and so that all payables can be paid and accounts receivable have been collected.
10. When the fiduciary's administration reaches its conclusion, the fiduciary should analyze which digital accounts should be terminated, and if any relevant content (or copies thereof) that have been obtained by the fiduciary should be deleted or (in an estate administration) distributed to the appropriate beneficiaries. The fiduciary should use care at this juncture to minimize the potential exposure of the user's identity to theft.

93 However, note that Section 6 of RUFADAA allows the custodian to utilize options that are short of full access to the digital assets in question.

94 Apart from RUFADAA's disclosure procedures, if a fiduciary lawfully obtains the means to access digital assets, and such assets are subject to the fiduciary's control, Section 15(d) of RUFADAA will likely shield the fiduciary from liability under state computer-fraud and unauthorized-computer-access laws. While RUFADAA is subject to federal preemption, the fiduciary's inherent authority under state law combined with RUFADAA Section 15(d) likely gives the fiduciary a good argument that such access is not "without authorization" or exceeds authorization under the CFAA, 18 USC § 1030(a).

VII. CONCLUSION.

In the last several decades, the "Information Age" has dramatically changed all aspects of our lives. With these changes, we have witnessed serious debates relating to individual privacy, and issues relating to the manner in

which both civil and criminal laws should be administered. In a world in which information vital to modern society is created, communicated, and stored on the Internet, it is inevitable that the traditional manner in which individuals undertake their estate planning must change and adapt.

RUFADAA is an example of this societal evolution. However, the act is an imperfect solution to many typical dilemmas that estate planners must solve. In the coming years, attorneys and other professional advisors will need to grapple with the manner in which federal statutes such as the SCA significantly impact both the interpretation of state statutes such as RUFADAA as well as a fiduciary's administration of digital assets. The courts, future state legislatures, and ultimately, Congress, will all need to continue to deal with the evolution of the law relating to digital assets.

Appendix A

Sample Will or Trust Language

(a) My Personal Representative may take any action (including, without limitation, assuming or amending a terms-of-service agreement or other governing instrument) with respect to my Digital Assets, Digital Devices, or Digital Accounts as my Personal Representative shall deem appropriate, and as shall be permitted under applicable state and federal law. My Personal Representative may engage experts or consultants or any other third party, and may delegate authority to such experts, consultants, or third party, as necessary or appropriate to effectuate such actions with respect to my Digital Assets, Digital Devices, or Digital Accounts, including, but not limited to, such authority as may be necessary or appropriate to decrypt electronically stored information, or to bypass, reset, or recover any password or other kind of authentication or authorization. This authority is intended to constitute "lawful consent" to any service provider to divulge the contents of any communication or record under the Stored Communications Act (currently codified as 18 USC § 2701, et seq.), the Computer Fraud and Abuse Act (currently codified as 18 USC § 1030), and any other state or federal law relating to Digital Assets, data privacy, or computer fraud, to the extent such lawful consent may be required. My Personal Representative shall be an authorized user for purposes of applicable computer-fraud and unauthorized-computer-access laws. The authority granted under this paragraph is intended to provide my Personal Representative with full authority to access and manage my Digital Assets, Digital Devices, or Digital Accounts, to the maximum extent permitted under applicable state and federal law and shall not limit any authority granted to my Personal Representative under such laws.

(b) The following definitions and descriptions shall apply under this will to the authority of the Personal Representative with respect to my Digital Assets and Digital Accounts:

(1) "Digital Assets" shall be any electronic record that is defined as a "Digital Asset" under the Oregon Revised Uniform Fiduciary Access to Digital Assets Act, together with any and all files created, generated, sent, communicated, shared, received, or stored on the Internet or on a Digital Device, regardless of the ownership of the physical device upon which the digital item was created, generated, sent, communicated, shared, received, or stored (which underlying physical device shall not be a "Digital Asset" for purposes of this will).

(2) A "Digital Device" is an electronic device that can create, generate, send, share, communicate, receive, store, display, or process information, including, without limitation, desktops, laptops, tablets, peripherals, storage devices, mobile telephones, smart phones, cameras, electronic reading devices, and any similar digital device that currently exists or may exist as technology develops or such comparable items as technology develops.

(3) "Digital Account" means an electronic system for creating, generating, sending, sharing, communicating, receiving, storing, displaying, or processing information that provides access to a Digital Asset stored on a Digital Device, regardless of the ownership of such Digital Device.

(4) For the purpose of illustration, and without limitation, Digital Assets and Digital Accounts shall include email and email accounts, social network content and accounts, social media content and accounts, text, documents, digital photographs, digital videos, software, software licenses, computer programs, computer source codes, databases, file sharing accounts, financial accounts, health insurance records and accounts, health care records and accounts, domain registrations, DNS service accounts, web hosting accounts, tax preparation service accounts, online store accounts and affiliate programs, and other online accounts that currently exist or may exist as technology develops, or such comparable items and accounts as technology develops, including any words, characters, codes, or contractual rights necessary to access such items and accounts.

Appendix B

Sample RUFADAA Disclosure Request Letter

Estate of Joseph Cordelia, Deceased
565 N. Edgar Drive
Portland, OR 97203
(503) 555-0122

November 18, 2017

Via Certified Mail 3419 9866 0430 0011 4755 38
Return Receipt Requested
Ingens Electronics
5656 Silicone Drive
Mionloch Acres, CA 94010

Re: Email Account of Joseph Cordelia, Deceased (jcordelia@ingens.com)

Dear Sirs:

I am the duly appointed personal representative of Joseph Cordelia (the "Decedent"). The Decedent died on September 14, 2017.

Pursuant to the Oregon Revised Uniform Fiduciary Access to Digital Assets Act, Section 7, Chapter 19, Oregon Laws 2016 (hereafter, "RUFADAA"), I hereby request full access to the email account maintained by Ingens Electronics. In connection with this request, I am enclosing the following:

1. A certified copy of the death certificate of the Decedent.

2. A certified copy of the Letters Testamentary issued by the Multnomah County, Oregon, Circuit Court on October 25, 2017, which appoints me as the personal representative of the Decedent's estate.

3. A copy of the Will of Joseph Cordelia dated July 27, 2014. Please note that pursuant to Section G of Article 7 of the Decedent's Will, the Decedent expressly provided his full consent to the disclosure of all his digital assets to his personal representative, and further authorized his personal representative to take any and all actions relating to his digital assets as his personal representative shall deem appropriate.

4. A copy of an email dated March 3, 2017, which was sent to me by the Decedent. This email contains the Decedent's ingens.com email address referenced above, together with other information identifying the Decedent's account with Ingens Electronics.

I look forward to your prompt response in accordance with RUFADAA. Please contact me if you have any questions.

Very truly yours,

Jane Cordelia, Personal Representative
Estate of Joseph Cordelia, Deceased

Firearms in Estate Administration Part II – NFA Firearms

Brian M. Thompson
The Law Office of Brian M. Thompson
Eugene, Oregon

There are numerous concepts that a person needs to understand when dealing with firearms during the planning and administration of a decedent's estate. This article will only deal with firearms regulated under the National Firearms Act of 1934[1] ("NFA"). Issues applicable to ordinary hunting and self-defense[2] firearms, and to firearms generally, were dealt with in a previous article. Gun trusts will be addressed in a third article.

The most important firearm concept is safety. Whenever a firearm is encountered, the four firearm safety rules[3] apply: **Rule 1:** All Guns Are Always Loaded; **Rule 2:** Never Let The Muzzle Cover Anything You Are Not Willing to Destroy; **Rule 3:** Keep Your Finger off the Trigger Until Your Sights Are on the Target and You Are Ready to Shoot; **Rule 4:** Be Sure of Your Target and Backstop.

Criminal Prosecution. Once we have made ourselves safe, the next issue is avoiding criminal prosecution. This article will give a short overview of the physical and/or mechanical characteristics of an NFA Firearm, the general requirements of ownership, and issues that may trigger criminal prosecution. This article will focus on how to avoid issues in estate planning and administration.

What Is an NFA Firearm? The NFA was passed in response to gangland crime of the Prohibition Era. NFA Firearms[4] include a much smaller subset of firearms, such as machineguns and silencers. It is important to note the definition of "firearm" under the NFA incudes items that are not firearms. Therefore, the term "NFA Firearm" is a term of art under the NFA and cannot be applied to any other state, local, or federal gun law.

An NFA Firearm is a firearm that requires special permission from the federal government to purchase, possess, own, and transfer. The NFA restricts and taxes:

- Short Barreled Rifles and Short Barreled Shotguns;
- Fully Automatic Weapons (machineguns, automatic rifles, and sub-machineguns);
- Suppressors/Silencers; and
- Items classified as Destructive Devices (grenades, mortars, etc.).[5]

The NFA imposes a tax of $200 on the transfer of NFA Firearms. This was a lot of money in 1934. However, the tax amount has not changed since 1934 and is no longer an obstacle to acquiring an NFA Firearm.

Procedure to Purchase an NFA Firearm. The procedure to purchase an NFA Firearm starts with the buyer paying for an item that is in stock at a gun shop. The buyer must then submit an application, filed in duplicate, with the $200 tax to the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"). This is generally referred to as a "Form 4."[6] Usually, the gun shop helps the buyer complete and file all of the paperwork. It takes three to six months for the form to be processed and a thorough

1 26 USC § 5801, *etseq.*

2 The right to firearms is specifically set out in the Oregon Constitution, article 1, section 27, which provides: "The people shall have the right to bear arms for the **defence** of themselves, and the State, but the Military shall be kept in strict subordination to the civil power." This reflects the fundamental human right of self-defense.

3 Excerpted from *The Modern Technique of the Pistol, by Greg Morrison, Gunsite Press, Paulden, Arizona, ISBN 0-9621342-3-6, Library of Congress Number 91-72644, $40.*

4 26 USC § 5845(a) ("The term 'firearm' means (1) a shotgun having a barrel or barrels of less than 18 inches in length; (2) a weapon made from a shotgun if such weapon as modified has an overall length of less than 26 inches or a barrel or barrels of less than 18 inches in length; (3) a rifle having a barrel or barrels of less than 16 inches in length; (4) a weapon made from a rifle if such weapon as modified has an overall length of less than 26 inches or a barrel or barrels of less than 16 inches in length; (5) any other weapon, as defined in subsection (e); (6) a machinegun; (7) any silencer (as defined in section 921 of title 18, United States Code); and (8) a destructive device. The term 'firearm' shall not include an antique firearm or any device (other than a machinegun or destructive device) which, although designed as a weapon, the Secretary finds by reason of the date of its manufacture, value, design, and other characteristics is primarily a collector's item and is not likely to be used as a weapon.").

5 ATF NFA Handbook (Apr. 2009), https://www.atf.gov/firearms/national-firearms-act-handbook.

6 ATF Form 5320-4. https://www.atf.gov/firearms/docs/form/form-4-application-tax-paid-transfer-and-registration-firearm-atf-form-53204/download.

background check completed.[7] The ATF will return the approved Form 4 with a NFA tax stamp affixed to it (an example is pictured below). The gun shop then completes a Form 4473 (described in detail in the September 2016 issue of the *Oregon Estate Planning and Administration Section Newsletter*) but DOES NOT request an additional background check. The Form 4473 is for internal gun shop bookkeeping purposes. The buyer may then take the NFA Firearm and the stamped Form 4 home.


V08502
Application for Tax Paid Transfer and Registration of Firearm

Note on Proof of Registration: The approved application received from the ATF serves as evidence of registration of the NFA Firearm. This document must be made available upon the request of any ATF officer. It is suggested that a photocopy of the approved application be carried by the possessor when the weapon is being transported.[8]

Short Barreled Rifles and Short Barreled Shotguns. An "ordinary" (non-NFA) rifle has a barrel 16 inches or longer. An "ordinary" (non-NFA) shotgun has a barrel 18 inches or longer. The overall length of either must be over 26 inches. A Short Barreled Rifle ("SBR") is any rifle with a barrel shorter than 16 inches. A Short Barreled Shotgun ("SBS") is any shotgun with a barrel shorter than 18 inches. Both SBRs and SBSs are regulated NFA Firearms.

NOTE: These barrel length and overall length requirements do not apply to handguns.

Measuring Barrel Length. Barrels are measured from a closed bolt. The measurement is *internal*. Barrels are measured by inserting a dowel rod into the barrel until the rod stops against the bolt or breech face. The rod is then marked at the furthermost end of the barrel or permanently attached muzzle device, withdrawn from the barrel, and measured.[9]

Fully Automatic Weapons (Machineguns). The term "machinegun" means any weapon that shoots, is designed to shoot, or can be readily restored to shoot, automatically more than one shot, without manual reloading, by a single function of the trigger. The term also includes: (i) the frame or receiver of any such weapon; (ii) any part designed and intended solely and exclusively, or combination of parts designed and intended, for use in converting a weapon into a machinegun; and (iii) any combination of parts from which a machinegun can be assembled if such parts are in the possession or under the control of a person.[10]

Machine guns are generally fully automatic weapons and are not commonly found in an ordinary estate's inventory. However, they are lawful to own and many people continue to seek approval to own them.

> **EXAMPLE:** The M1 Carbine was used in World War II and the Korean War. The M1 Carbine is not a fully automatic weapon (and not an NFA Firearm). However, between World War II and the Korean War, the United States military created a conversion kit that converted the M1 Carbine into a fully automatic rifle—the M2 Carbine. The M2 Carbine, the M2 Carbine conversion kit, and a single part of the M2 Carbine conversion kit are regulated under the NFA.

Many of the M1 Carbines and M2 Carbines were sold by the United States to other governments. They ended up in Vietnam, Africa, and South America. Che Guevara is carrying an M2 Carbine in the photo to the right. Some of these M2 Carbines and M2 Carbine conversions and/or conversion kits found their way back into the United States.

7 This is much more thorough than the National Instant Criminal Background Check necessary for the transfer of a non-NFA Firearms as discussed in the September 2016 issue of the Estate Planning Newsletter.

8 26 USC § 5841(e); 27 CFR § 478.101.

9 ATF NFA Handbook § 2.11.

10 26 USC § 5845(b).

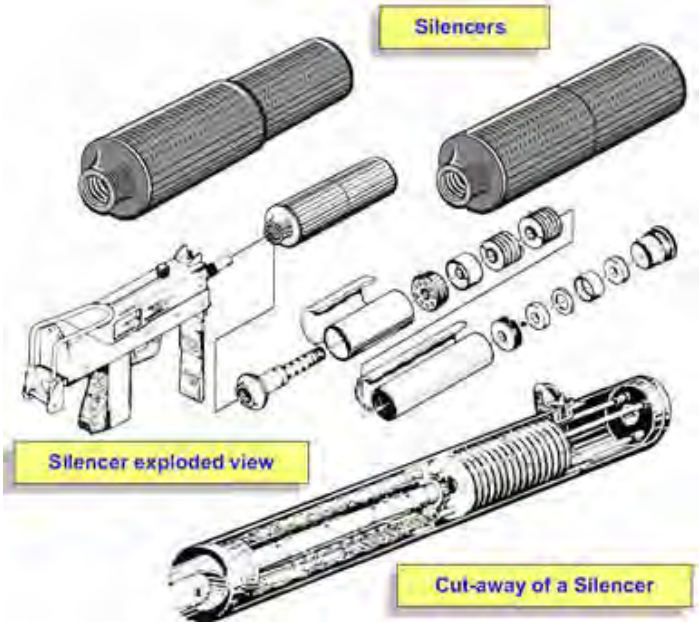
Below is a combination of parts (a "kit") that can convert an M1 Carbine into an M2 Carbine. This combination of parts is regulated as if it were a machinegun.

The photo below shows a single part of the "kit" that can convert an M1 Carbine into a machine gun. This single part is also regulated as if it were a machinegun.

Parts like these, although rare, might be found in an estate.

Silencers/Suppressors. Silencers are most commonly referred to as suppressors. Often people will refer to a weapon as "suppressed" (example: "My 300 Blackout is suppressed"). This implies that there is a suppressor on the weapon. Suppressors are becoming more and more common and may be encountered in an estate.

Silencers/suppressors are also regulated by the NFA, defined as "any device for silencing, muffling, or diminishing the report of a portable firearm, including any combination of parts, designed or redesigned, and intended for use in assembling or fabricating a firearm silencer."[11]



Destructive Device. The category of destructive devices includes explosive devices (grenades, bombs), large caliber weapons (mortars and cannons), and other weapons including rocket propelled grenades.[12] However, the definition does not include antique firearms such as a Civil War cannon.[13] These items are not common and are generally owned only by sophisticated collectors. However, certain firearms are also regulated as destructive devices, such as the USAS-12 (a 12-gauge shotgun produced in South Korea and used primarily for military and law enforcement). See photo below.

Exceptions That Prove the Rule. As with any regulatory scheme, there are exceptions based upon historical practice and technological innovation. Examples of each are described below.

Any Other Weapon Exception. The NFA was passed in 1934. This was the middle of the Great Depression. Many firearms that were in use in the country at that time violated the barrel length and stock length requirements. Most of these weapons were foraging weapons. An example would be the Marbles Game Getter, shown below.

11 18 USC § 921(A)(24) ("The terms 'firearm silencer' and 'firearm muffler' mean any device for silencing, muffling, or diminishing the report of a portable firearm, including any combination of parts, designed or redesigned, and intended for use in assembling or fabricating a firearm silencer or firearm muffler, and any part intended only for use in such assembly or fabrication.").

12 26 USC § 5845(f).

13 *Id.*; *see also* ATF NFA Handbook § 2.1.8.

This firearm is intended to be carried on a horse pack or on a plow and used to forage for rabbits or squirrels.

Therefore, an exception was introduced to the NFA for what is defined as "Any Other Weapon."[14] Section 2.1.5 of the ATF NFA Handbook lists some of the other exemptions.

The "Any Other Weapon" category is a catch-all for odd weapons that are not readily categorized. The tax is only $5, but the Form 4 and tax stamp are still required. The Serbu Super Shorty (below) is also treated as an Any Other Weapon.

Modular Weapons. Many firearms can be configured for different applications. The Thompson/Center Arms

Company manufactured a weapon that was modular. Barrels could be attached and removed in either rifle or pistol length. A pistol grip or a rifle stock could be installed. The primary purpose of the Thompson/Center firearm was the pursuit of a type of shooting competition that was popular in the 1970s and 1980s. This competition required multiple handguns and rifles in order to compete. The Thompson/Center firearm allowed a person to own just one firearm and a few attachments. This reduced the cost dramatically. A pistol grip and pistol barrel could be installed and used for a pistol competition. Later in the same day, the pistol grip and pistol barrel could be swapped out and the rifle stock and rifle barrel could be installed for a rifle competition. The photo below displays ONE Thompson/Center firearm and several different barrels and stocks.

The ATF took issue with the design and the fact that the company sold the pistol/rifle as a kit. The ATF argued

that the purchaser could easily build a prohibited weapon by simply installing a pistol barrel on the rifle stock. This would create an SBR. Therefore, the ATF argued, the weapon was illegal to sell. The U.S. Supreme Court disagreed.[15] The court ruled that the mere potential for illegal assembly was not a valid reason to restrict sale of the weapon. End users who constructed an illegal weapon would be held liable for their actions, however.

One of the military advantages of the AR15 style rifle (a non-NFA Firearm) is its modular nature. The AR15 can also be configured as either a rifle or a pistol—both of which are lawful, non-NFA Firearms. Many clients will have short barreled AR15 "uppers" that attach to AR15 pistol "lowers." This is perfectly lawful. However, it is illegal to attach an AR15 pistol upper to an AR15 rifle lower. This will create an SBR (an NFA Firearm).

NFA Firearms in an Estate. New federal regulations were issued effective July 13, 2016. 27 CFR pt 479. This is the first time that a personal representative has been specifically authorized to work with the decedent's NFA Firearms. Trustees of revocable trusts are not authorized

14 26 USC § 5845(e) ("The term 'any other weapon' means any weapon or device capable of being concealed on the person from which a shot can be discharged through the energy of an explosive, a pistol or revolver having a barrel with a smooth bore designed or redesigned to fire a fixed shotgun shell, weapons with combination shotgun and rifle barrels 12 inches or more, less than 18 inches in length, from which only a single discharge can be made from either barrel without manual reloading, and shall include any such weapon which may be readily restored to fire. Such term shall not include a pistol or a revolver having a rifled bore, or rifled bores, or weapons designed, made, or intended to be fired from the shoulder and not capable of firing fixed ammunition.").

15 *United States v. Thompson/Center Arms Co.*, 504 US 505 (1992).

under these regulations. The rules governing trustees will be discussed in the article about gun trusts.

- 27 CFR § 479.90(a) (a) The personal representative in an estate may possess a firearm registered to a decedent during the term of probate without such possession being treated as a "transfer" under the NFA. No later than the close of probate, the executor must submit an application to transfer the firearm to beneficiaries or other transferees in accordance with this section. If the transfer is to a beneficiary, the executor shall file an ATF Form 5 (5320.5), Application for Tax Exempt Transfer and Registration of Firearm (a tax-free transfer).
- (c) The personal representative in an estate shall submit with the transfer application documentation of the person's appointment as personal representative, a copy of the decedent's death certificate, a copy of the will (if any), any other evidence of the person's authority to dispose of property, and any other documents relating to or affecting the disposition of firearms from the estate.

Estate Example 1: Decedent lived in Portland, Oregon. Decedent owned numerous ordinary firearms and a suppressor (an NFA Firearm). Decedent and Spouse resided in family home for decades. Spouse will continue to reside in family home. Spouse is the personal representative of the estate. Decedent's Will directs that the Decedent's firearms and related items are to be divided among the children at the discretion of the personal representative. Child One lives in San Diego, California. Child Two lives in Hawaii. Child Three lives in Bend, Oregon. Local laws of each child's residence will still apply. Therefore, the suppressor CANNOT go to Child One or Child Two—suppressors are illegal in California and Hawaii. Child Three agrees to take the suppressor.

Estate Procedure:

- Personal representatives are NOT required to have estate firearms registered to them prior to distribution to lawful heirs—simply being appointed by a court in a probate matter is sufficient.
- The personal representative must retain possession of the NFA Firearm (the suppressor) until approval for the transfer is granted by the ATF and the probate court. In this case, Spouse is the personal representative. Therefore, the NFA Firearm will not be moved to another location during the probate.
- When the Final Account and a proposed General Judgment of Distribution are filed, the proposed judgment should include a specific distribution of the NFA Firearm to Child Three. The Proposed Order should specifically list the NFA Firearm by model and serial number.
- When the General Judgment of Distribution is signed, ATF Form 5 must be filed by the personal representative to register the NFA Firearm to Child Three. Child Three will submit fingerprints on FBI Form FD-258 (which must accompany the transfer application). The form should also be accompanied by documentation showing the personal representative's authority to distribute the NFA Firearm as well as Child Three's entitlement to the NFA Firearm. This is why the General Judgment of Distribution must be signed.
- Distributions to Child Three should not be made until the Form 5 is approved. It will take three to six months to get approval.
- Once Form 5 is approved the personal representative may transfer the NFA Firearm to Child Three.
- The transfer should take place before the Supplemental Judgment is filed and the probate is closed.[16]

Estate Example 2: Decedent lived in Portland, Oregon. Decedent's Spouse predeceased Decedent. Decedent owned an SBR. Child Two is the personal representative of the estate. The Will directs that the Decedent's firearms and related gear are to be divided among the children at the discretion of the personal representative. Child One lives in Boise, Idaho. Child Two lives in Beaverton, Oregon. Child One would like the SBR, but only if Child One's suppressor will fit onto the SBR.

Estate Procedure:

- May Child Two take the SBR to Child One's home in Boise? Yes, but only after completing ATF Form 5320.20—commonly referred to as a "Form 20" (Application to Transport Across State Lines).[17]
- May Child One bring his suppressor from Boise to Beaverton? Yes. There is no requirement to file a Form 20. Suppressors and Any Other Weapon items can move across state lines without permission from the ATF. Note that all local laws must still be obeyed.
- Child Two is personal representative. May Child Two, as the personal representative, take possession of the SBR and keep it in Beaverton for the duration of the probate proceeding? Yes. If the SBR stays inside Oregon there is no requirement that the ATF

16 *See* ATF NFA Handbook § 9.5.3.1.

17 ATF Form 5320.20, https://www.atf.gov/resource-center/docs/atf-f-5320-20pdf-0/download.

be notified.[18] If the personal representative wishes to notify the ATF, the personal representative may do so using the Form 20. A good reason to notify the ATF may be the sale of the Decedent's home. The Decedent's address is associated with the suppressor. If a criminal event were to occur at Decedent's address (arson, burglary, etc.) the ATF might send an investigator. Having all of the i's dotted and the t's crossed will be comforting for the personal representative.

Sale of the NFA Firearm. If there are no beneficiaries of the estate who want the NFA Firearm, the personal representative may dispose of the item outside the estate (most likely by selling it).[19] Professional assistance should be obtained when selling an NFA Firearm. The labyrinth of federal, state, and local laws and the selection of proper ATF forms are beyond the scope of this article.[20]

Uncertainty About the Registration of Decedent's Firearms. If the decedent's NFA Firearms are not registered to him/her in the National Firearms Transfers Record, the firearms are contraband and may not be lawfully possessed or transferred. If the personal representative cannot locate the decedent's registration documents, he/she should contact the local ATF field office in writing and inquire about the firearms' registration status.[21] The inquiry should include letters of testamentary and other documentation as set forth in ATF NFA Handbook § 9.5.3.3.

Such uncertainty is not uncommon. In 2014, a World War II fully automatic firearm (valued in excess of $30,000) was turned in to a gun buyback program in Hartford, Connecticut. A police officer with the Hartford Police Department recognized the weapon and saved it from destruction. The person who brought in the firearm was the child of a World War II veteran. The veteran simply brought it home as a souvenir. The firearm was never registered and was technically in violation of the NFA. However, the daughter dealt with it responsibly (by turning it in) and she was not prosecuted. The firearm was a rare collector's piece (a Sturmgewehr!) and ended up in a firearms museum due to its rarity and historical significance.

Destruction of an NFA Firearm. In the event a family member or the personal representative decides to destroy an NFA Firearm, specific guidelines must be followed. An example would be an older suppressor/silencer. These wear out with use and may have no market value. ATF NFA Handbook § 2.5 notes that a machinegun receiver and all the components of a silencer must be destroyed. The preferred method for destroying a machinegun receiver is to completely sever the receiver in specified locations by means of a cutting torch that displaces at least a quarterinch of material at each cut location. The emphasis is on complete destruction of the item so that it may not be welded together later. An item that is not properly destroyed may still be classified as an NFA Firearm—and all of the NFA rules and criminal penalties will still apply.

Conclusion. NFA Firearms include a small subset of firearms, such as SBRs, SBSs, machineguns, and suppressors/silencers. State and local laws applicable to ordinary hunting and self-defense firearms, and to firearms generally, usually apply. In addition, state and local laws may specifically address (or even prohibit) some NFA Firearms. Attorneys working with estates that include NFA Firearms should be cautious and not be afraid to retain expert help as needed. This will help avoid hiring a different expert—a criminal defense attorney—after a mistake is made.

18 **Change of Address. 18 USC § 922(a)(4) ("It shall be unlawful ***** for any person, other than a licensed importer, licensed manufacturer, licensed dealer, or licensed collector, to transport in interstate or foreign commerce any destructive device, machinegun (as defined in section 5845 of the Internal Revenue Code of 1986), short-barreled shotgun, or short-barreled rifle, except as specifically authorized by the Attorney General consistent with public safety and necessity[.]").

19 27 CFR § 479.90a(b) ("If there are no beneficiaries of the estate or the beneficiaries do not wish to possess the registered firearm, the executor will dispose of the property outside the estate (i.e., to a non-beneficiary). The executor shall file an ATF Form 4 (5320.4), Application for Tax Paid Transfer and Registration of Firearm, in accordance with § 479.84.").

20 *See* ATF NFA Handbook § 9.4.2.

21 Local ATF field offices can be found at https://www.atf.gov/contact/atf-field-divisions.

Events Calendar

46th Annual Estate Planning Seminar

What: Estate Planning CLE sponsored by the Estate Planning Council of Portland, Inc.

When: January 20, 2017

Where: Oregon Convention Center, Portland

The Editors want to include announcements of upcoming events that are open to the public and may be of interest to our readers. If you know of an event, please send basic information, including point of contact information to Sheryl S. McConnell at *Sheryl@mcconnellattorney.com* for inclusion in the next issue of the Newsletter.

Tangible Letters: Gifts Made by a Writing Other Than a Will

Anne Villella
Professor, Lewis & Clark Law School
Attorney, Pariani Villella, LLC
Portland, Oregon

If you have handled even a small number of probates, no doubt you have had the personal representative report that the testator affixed labels or masking tape to personal effects identifying who should receive them. Of course, the will or intestate succession controls the disposition of tangible personal property, not labels or masking tape.

To reduce circumstances such as the above, for many years attorneys have included "written list provisions" in wills that allow testators to leave a writing identifying items of tangible personal property and the devisee who is to receive each item; however, such writings are not binding because they lack the formalities required for the execution of a will. As such, attorneys have drafted written list provisions using precatory language directing the personal representative to honor the testator's wishes, but not binding the personal representative.

This article alerts practitioners to the requirements of ORS 112.260, which became effective January 1, 2016. Specifically, ORS 112.260 allows the testator to create a writing and requires the personal representative to honor it, provided the writing complies with the statute. By enacting ORS 112.260, the legislature created a means to honor a testator's wishes even though a writing does not otherwise comply with the Wills Act.

Since many practitioners have used written list provisions that were non-binding, reviewing and revising those provisions may be in order because of the specific statutory requirements of ORS 112.260. Specifically, unless the will provides otherwise, ORS 112.260 permits a testator to leave a written statement or list—which is admissible as evidence of the testator's intended disposition of tangible personal property—provided the writing:

- Is referred to in the testator's will;
- Is signed by the testator;
- Describes the items of tangible personal property with reasonable certainty; and
- Describes the devisee with reasonable certainty. ORS 112.260(2)(a)-(c).

In addition, ORS 112.260 limits the type of property a testator may dispose of using a writing referred to in a will. Under ORS 112.260(1), the testator may dispose of household items and personal effects, but the testator may *not* use the writing to dispose of "[m]oney, property used in trade or business," or "items evidenced by documents or certificates of title." ORS 112.260(1). Thus, advising a client about leaving personal effects to specific devisees requires educating the client that specific gifts of items, such as vehicles, bank accounts, securities, or tangible personal property used by the testator in his or her business, *must* be made by will, not by a writing under ORS 112.260.

ORS 112.260(3) permits the use of a writing "prepared before or after the execution of the testator's will," so long as it is "in existence at the time of the testator's death." Moreover, the testator may change the writing over the course of time. ORS 112.260(4).

Finally, the statute defines a "writing" as including an electronic record, document, or image. ORS 112.260(5). This language is contrary to the provisions for the execution of a will under ORS 112.235(4), which defines a "writing" as *not* including an electronic record, document, or image. Although it is unclear precisely what the drafters had in mind regarding this definition of a "writing" in ORS 112.260, it necessarily does away with the strict writing requirements for the execution of a will under ORS 112.235. Indeed, the definition seems to contemplate that in addition to a paper document, an electronic record or image would be admissible. Because the statute does not define what "signed by the testator" means, it is unclear whether the drafters considered whether ORS 112.260 would encompass a digitally *signed* writing.

What should a provision in the will include? Although ORS 112.260 differs from the UPC in some respects, the following sample provision from the Comment to UPC 2-513 is consistent with ORS 112.260:

> I might leave a written statement or list disposing of items of tangible personal property. If I do and if my written statement or list is found and is identified as such by my Personal Representative no later than 30 days after the probate of this will, then my written statement or list is to be given effect to the extent authorized by law and is to take precedence over any contrary devise or devises of the same item or items of property in this will.

The UPC sample clarifies that the writing controls disposition of listed items if the personal representative finds the writing within 30 days of the opening of probate. It also clarifies that the testator's intent that a specific gift of an item of tangible personal property made by a signed writing controls disposition, *even if a contrary gift appears in the will.*

When drafting a written list provision, the attorney might also consider whether to address the following:

- If multiple lists are found, which list takes priority;
- If the same item is given away in different lists to different people, which gift takes priority; and

- If the written list is not binding because it does not comply with the statute or was found later, whether to request that the personal representative and beneficiaries follow the testator's wishes.

From a practice standpoint, ORS 112.260 seems to contemplate that the written list may be filed with the will because it is admissible as evidence of the testator's intent. However, it may make sense to file the writing as evidence of the testator's intent only in those circumstances that warrant it. For example, the writing should be submitted along with the will if the writing includes gifts of items to an individual who is not otherwise a devisee under the will. Similarly, if the writing names individuals who are named in the will as recipients of tangible personal property, submitting the writing to the court as evidence of the testator's intent makes sense when those receiving tangible personal property dispute the testator's intent regarding distribution of those items.

In sum, the statute creates an opportunity for clients to leave specific gifts of tangible personal property by a writing that lacks the formalities required for wills, yet binds the personal representative. However, practitioners must draft the written list provision to make such lists binding and educate clients regarding the statutory requirements. As with any document that has formality requirements—even the few required under ORS 112.260—there is always the risk that the testator will fail to satisfy the statutory requirements. However, if the statutory requirements are not met, the harmless error rule under ORS 112.238 or the doctrine of incorporation by reference under ORS 112.255(3) might save the writing if the requirements for those provisions are met. Similarly, as has been the practice before, a personal representative and beneficiaries may honor the testator's wishes, even if not bound to do so.

The Jeffrey M. Cheyne Memorial Service Award

The Jeffrey M. Cheyne Memorial Service Award, named after the late Jeffrey M. Cheyne, an Oregon estate and trust attorney who contributed significantly to the advancement of Oregon estate planning and administration, legislation, and attorney education and mentoring, was established in 2016 by the Estate Planning & Administration Section of the Oregon State Bar to honor those individuals who demonstrate significant long-term commitment, service, and contributions to the Oregon estate planning and probate/trust administration community.

The first recipient is Jeffrey M. Cheyne, posthumously. The award will be accepted by his wife, Debra Cheyne.

Oregon Estate Planning and Administration Section Newsletter

Editorial Board

Janice Hatton
Philip N. Jones
John D. Sorlie
Timothy R. Strader
Vanessa Usui
Michele Wasson

Questions, Comments, Suggestions About This Newsletter?

Contact: Sheryl S. McConnell, Editor-in-Chief

(503) 857-6860 Sheryl@mcconnellattorney.com