Bloomberg BNA

Electronic Commerce & Law Report™

VOL. 19, NO. 19 MAY 14, 2014

Payments

Bitcoin Is Creating New Headaches for Estate Planners, Though It May Someday Cure Them

For attorneys and state legislators, who are only now working through new legal issues created by the prior decade's digital output, the emergence of bitcoins and other virtual currencies is creating additional, and unique, challenges.

To date, very few lawmakers have focused on the challenges that virtual currencies create for estate planning attorneys and the fiduciaries who act on behalf of decedents and their estates. Fortunately, the technology behind Bitcoin may allow savvy estate planners and clients to solve some of those problems ahead of time.

Traditionally, fiduciaries and family members would go through the deceased's belongings and watch the mail for important financial documents. Now, many of those belongings and documents might be contained on a hard drive, in an e-mail account, or in cloud storage. They include things such as online bank accounts, electronically delivered bank statements, iTunes purchases, Facebook photos and e-mail accounts.

Additional obstacles arise when fiduciaries attempt to access the digital assets left behind by the deceased: passwords, encryption, unauthorized access and computer crime laws, and privacy laws. Passwords and encryption are technological roadblocks to accessing information, while unauthorized access and privacy laws put fiduciaries and trusts and estates lawyers at risk of violating one set of laws simply for attempting to perform the duties required under another set of laws.

In this article, the capitalized term ''Bitcoin'' refers to the technology in general, while the lowercase ''bitcoin'' and ''bitcoins'' refer to individual units of currency, such as dollars.

Statutory Obstacles. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, creates civil and criminal liability for accessing protected computers, systems or networks without authorization or in excess of authorization and thereby obtaining information, including financial information. ''Exceeds authorized access'' is an imprecisely defined term; the CFAA does not specify which kinds of authorization are sufficient to created authorized access. The Ninth Circuit, for instance, has taken a pragmatic dictionary definition approach where any permission creates authorized access. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009) (14 ECLR 1358, 9/23/09).

Authorized access frequency does not extend beyond the account. Many service providers such as Facebook do not allow third parties to use someone else's login information under their terms of service. A fiduciary using a password the decedent left behind to log in to their Facebook account to download pictures is violating those terms, creating potential CFAA liability.

The Department of Justice has taken and defended the legal position that violations of a service provider's terms of service are actionable under the CFAA (16 ECLR 1909, 11/23/11). While the DOJ does not routinely prosecute run-of-the-mill terms of service violations, the potential to do so looms over fiduciaries and counsel who are merely attempting to perform their duties to the decedent's estate.

Bitcoin exchanges have a startup mentality focused on operations and technology without necessarily developing the legal and policy infrastructure of a more experienced financial firm.

Service providers are incentivized under federal law to put up such barriers. The Stored Communications Act, 18 U.S C. § 2701, a portion of the Electronic Communications Privacy Act, prohibits computer service provider from disclosing the contents of users' electronic communications without their lawful consent. As with authorization under the CFAA, ''lawful consent'' under the SCA is undefined, and the law is not well-developed around fiduciaries. Also, the ''lawful consent'' provision is merely permissive: providers may provide access but are not required to do so. Because the SCA puts service providers at risk, providing no access at all can often be a safe default position.

Uniform Law Proposal. The Uniform Law Commission has recognized the difficulty of dealing with digital assets post-mortem, and in 2011 it created the Fiduciary Access to Digital Assets committee (18 ECLR 349, 2/20/13) in a response to a proposal co-authored by

 ISSN 1098-5190

Gray Plant Mooty estate planning partners Gene Hennig and James Lamm. In March 2014 that committee issued its fifth draft of a proposed Fiduciary Access to Digital Assets Act (FADAA). The commentary to that draft specifies that ''digital assets include digital currency and similar products currently in existence and yet to be invented.''

''The [draft] Act is to clarify law, not forging new ground,'' Lamm said. Longstanding fiduciary laws exist that allow a representative to stand in the shoes of the deceased individual for recovering real or tangible property, Lamm said, and the FADAA is meant to clarify that those laws also apply to digital assets.

The FADAA attempts to shield fiduciaries and the service providers they correspond with from liability. ''By defining the fiduciary as an authorized user: 1) the fiduciary has authorization to access the files under the first section of the SCA, 18 U.S.C. § 2701, as well as under the CFAA; and 2) the fiduciary has ''the lawful consent'' of the originator/subscriber so that the provider can voluntarily disclose the files pursuant to the second relevant provision of the SCA, 18 U.S.C. 27 § 2702,'' the current draft states. ''Moreover, this language should be adequate to avoid liability under the state unauthorized access laws.''

The FADAA addresses four types of fiduciaries: personal representatives, conservators, agents operating under power of attorney, and trustees.

While slight differences apply to each type of fiduciary under the latest draft, for each the FADAA authorizes access to all digital assets except the content of communications, and access to the content of communications to the extent service providers are permitted to disclose them under the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq.

Fiduciaries receive several protections under Section 8 of the FADAA. Any of the above-listed fiduciaries may take action concerning the asset with the same level of authority as the decedent asset holder, subject to other law and terms-of-services agreements. Fiduciaries are also defined under this section as ''authorized users'' under the CDAA and as having ''lawful consent'' of the account holder for custodians to divulge electronic communications to them. Fiduciaries with authority over decedents' electronic equipment are also expressly authorized to access the equipment and electronic records stored on it.

Custodians also receive protection under Sections 9 and 10. Section 9 describes the procedures required by fiduciaries in order to access digital assets, requires custodians to comply with requests and provides a 60-day compliance timetable. Section 10 provides that custodians are immune from liability for good faith compliance. Section 9(f) also allows custodians to rely on certifications of trust without further inquiry.

The Drafting Committee memo to the most recent draft suggests that Sections 8(b) and (c) are primary remaining sticking points. Those provisions state that fiduciary access is not a terms-of-services violation despite any provision to the contrary and that fiduciary access limitations in terms-of-services agreements are void as against public policy unless those provisions are signed separately from the other provisions of the agreement.

How Bitcoins Are Held. Returning to the topic of bitcoins, an understanding of virtual cryptocurrencies is critical to understanding how an executor might locate and acquire the decedent's bitcoins.

Bitcoin uses public key encryption that requires combining public and private keys to create a transaction. Public keys are stored on a cloud-like system known as the blockchain, that also serves to verify transactions through distributed computing power. To complete the transaction, the owner of the bitcoin must supply the private key to combine with the public key to ''sign'' the transaction.

Bitcoins lack any physical embodiment. Transactions are recorded on, and the value of bitcoins comes from, a distributed technology called the blockchain. The blockchain is similar to a chain of title, a full asset ledger similar to a grantor-grantee list, anonymized via encryption.

Instead, bitcoins can be held in three forms—on a wallet tied to an exchange, in a wallet maintained by the holder, or in cold storage. A wallet is basically software that provides an interface for using bitcoins. Bitcoins held in an exchange wallet are subject to the terms and conditions of the exchange. In that instance, the exchange maintains possession of the private key. A hacker gaining access to the exchange's servers could steal the user's private key and access their account in that way, as happened with the high-profile Mt. Gox data breach (19 ECLR 299, 3/5/14).

Bitcoin in a wallet maintained by the holder means only the bitcoin holder has the private key, which they can keep on one or more devices. The only way a hacker could gain access to bitcoin held in this way is by hacking into the individual's device, rather than a centralized repository.

''Cold storage'' is a special case of a wallet whose holder only maintains a paper copy of the private key, usually containing a long string of letters and/or a QR code, or maintains the key on a non-connected hard drive. Cold storage private keys are hack-proof, except by decidedly low-tech ''hackers'' such as fire, wind, magnets and rain.

The general recommendation in the Bitcoin community, Lamm said, is that any significant value of bitcoins should be held in cold storage the majority of the time, and only moved online in order to engage in transactions. Lamm said he recommends that all valuable data, including bitcoin private keys, should be stored in multiple places, whether that means hard drives, paper, or in the cloud.

Without a private key, bitcoins aren't lost per se, but they become permanently inaccessible. In this way, Lamm said, bitcoins are like chattel property that is unretrievable if physically lost. Thus a bitcoin holder (or their heir) without a private key is, well, bit out of luck.

Lamm recommended that fiduciaries and heirs who believe the deceased may have held bitcoins search hard drives for wallet software such as Bitcoin Core, Multibit, Hive or Armory. He also suggested searching mobile devices for popular wallet apps such as Bitcoin wallet, Mycenium, Blockchain or Kipochi. Also, browser history or bookmarks can contain links to online wallets and exchanges such as Coinbase, Blockchain or Strongcoin.

Contacting Exchanges. If evidence is found that the decedent maintained an online wallet with a Bitcoin exchange, the next step would be to contact the exchange just as you would about any other financial account.

When attempting to contact a bitcoin exchange that may not have a written policy on accountholder succession or even easily accessible customer service contact information, Lamm said fiduciaries can start by contacting the Secretary of State office wherever the exchange is incorporated to find the agent for service of process. Through that agent the fiduciary can pursue traditional legal remedies for claiming decedent assets.

Bitcoin exchanges are by definition relatively young companies, and co-Vice Chair of the Bitcoin Foundation Education Committee Pamela Morgan told Bloomberg BNA they often have a startup mentality focused on operations and technology without necessarily developing the legal and policy infrastructure of a more experienced financial firm.

''As these companies grow, it can be challenging to identify agents or principals of the companies,'' Morgan said. ''Also, many of these companies are incorporated outside the U.S. and without a true headquarters but operated through virtual offices all around the world.''

By contrast, executors can close PayPal accounts of deceased account holders by faxing a request to close the account along with a death certificate, photo ID of the executor and a copy of the will or other proof of the executor's authority to the company, a spokesperson told Bloomberg BNA. PayPal then reviews the documentation, closes the account, and sends the executor a check issued in the account holder's name.

Nevertheless, Morgan, whose firm Empowered Law handles Bitcoin-related matters, said her professional dealings with exchanges have ultimately been positive. ''I've found many of these companies rapidly responsive to legal issues once I'm able to identify the appropriate person.''

Bitcoin and the FADAA. How well equipped the draft FADAA is to handle Bitcoin issues remains an open question.

The draft FADAA focuses on giving fiduciaries legal access to the electronic records that represent the digital assets, Christina Kunz, Professor Emerita at the William Mitchell College of Law told Bloomberg BNA. Access to registry information that allows fiduciaries to find the relevant custodian of records even if they do not have the relevant private key is the primary concern of the drafters, said Kunz, who is the ABA Business Law section's observer to the drafting committee.

Kunz agreed with Lamm that the intent of FADAA drafters is similar to that of the drafters of the Uniform Electronic Transactions Act—to level the playing field between online commerce and ''bricks and mortar'' assets.

But Bitcoin may be a thorn in the committee's side, because it seems to be a case where the electronic record and the digital asset merge—the blockchain ''ledger'' is both the record of the asset and its essence. And the decentralized nature of the blockchain means there's no centralized authority when it comes to locating a solitary custodian, particularly for bitcoins not held in an exchange-connected wallet.

''If Bitcoin is a spread-out registry, maybe we haven't solved that issue,'' said Kunz.

The sixth draft of the FADAA is expected to be released before the ULC's summer meeting, which begins July 11 in Seattle, where it will get a second full reading and may be put to a vote.

Smart Contracts Solution? Until and unless the law adapts to Bitcoin succession issues, Bitcoin holders and their counsel might want to consider planning ahead using the very blockchain technology that powers Bitcoin to create smart contracts. Smart contracts are an application of Bitcoin's blockchain technology distinct from the currency aspect.

''Contracts'' in the Bitcoin community are more akin to what lawyers would call transactions, and smart contracts are self-executing transactions that transfer bitcoins once certain pre-programmed conditions have been met.

Mike Hearn, Bitcoin core developer and Chair of the Bitcoin Foundation's Law & Policy committee, described in 2012 how the blockchain could be used to automate a bitcoin conveyance through an ''external state contract.'' In his example, an elderly grandfather living in Missouri decided he wanted to give his grandson an inheritance upon his death or the grandson's 18th birthday, whichever came first. He did this by creating the infrastructure of a bitcoin transfer from his account to the grandson's, leaving the transaction complete except for his private key signature.

The private key signature would have been provided by whichever of two automated processes was completed first.

The grandfather first created a bitcoin ''contract'' using a ''LockTime'' function that would sign the transaction allowing the transfer of funds at the instant the grandson turned 18. The LockTime function would sign at that moment but no sooner.

The second part of the process was an external state contract, meaning a contract tied to information the blockchain cannot know, in this case whether a person was alive or dead. External state contracts require an ''oracle'' — a human or automated function instructed to ''sign'' the transaction as soon as a necessary condition is met — namely proof of death. As an automated function, the oracle could be a program that checks the state's online certificate of death database at a predetermined interval, and as soon as the grandfather appears in the database, signs the transaction. The oracle could also be a third-party individual given the authority to sign the transaction upon learning of the grandfather's death, either as part of a larger fiduciary role in the estate or as a paid third-party neutral, but who had no other role in the transaction, such as holding the funds like a traditional escrow agent.

Once the LockTime function or the external state contract completed the grandfather's side of the transaction, the grandson could sign using his own private key at any time. He could have signed before that, but the transaction would not be completed until the grand-

father's signature was provided by one of the two contracts.

Hearn told Bloomberg BNA that the grandfather could also use an external state contract to transfer the remaining contents of a ''live'' wallet, as opposed to a pre-determined sum, to the grandson. A harder case is presented, however, in a scenario in which the remaining contents of a live wallet must be split between four heirs. Doing so at present would be ''either tricky, inefficient, or downright impossible,'' Hearn said, because ''the wallet software would have to know about that and try to rebalance the bitcoins internally so they're distributed across four sets of keys which would dramatically increase complexity inside the wallet.'' Future upgrades to the Bitcoin protocol, however, could make this possible.

Hearn was less sanguine about an external state contract having the capacity to direct the remaining contents of a bitcoin wallet to pay the expenses of estate administration with the residue transferring automatically to heirs.

''That might be harder,'' he said. ''To impose ordering on such things without trusting the liquidator of the estate—not sure how to do that, as neither Bitcoin nor the grandfather can necessarily know what the expenses truly are.''

BY JOSEPH WRIGHT

To contact the reporter on this story: Joseph Wright in Washington at jwright@bna.com

To contact the reporter on this story: Thomas O'Toole in Washington at totoole@bna.com

  ECLR ISSN 1098-5190