South Carolina Bar
Continuing Legal Education Division

2024 SC BAR CONVENTION

Technology

"Technology & Law"

Saturday, January 20

SC Supreme Court Commission on CLE Course No. 240035

South Carolina Bar
Continuing Legal Education Division

2024 SC BAR CONVENTION

Technology

Saturday, January 20

A.I. Oh My!

Stuart Teicher

stuartteicher esq
I teach lawyers

CLE Performer & Ethics Educator
stuart.teicher@iCloud.com
www.stuartteicher.com
732-522-0371
East Brunswick, NJ

Oh My! The Ethics of Chat GPT and Other AI
Program Written Materials

So you've heard of this Chat GPT thing? I guess that means we should talk about it. Of course, this program isn't only about Chat GPT. To properly understand the ethics issues in that program, we actually have to go a little deeper. So in this program we'll be talking about the different ethics issues that impact both Chat GPT, artificial intelligence (generally), and a few other new technologies that are relevant to the discussion of generative AI.

1. The more things change, the more they stay the same.

a. Yesterday's standard.

There are a myriad of technologies being used in the practice of law today. Whether it's email, texting, cloud storage, software as a service (SaaS), or artificial intelligence in its many forms, there's one common concern. With each technology we are moving data. Whether we are moving data from one person to another or moving it into the cloud, moving it to a software system so that system can process the data, it doesn't matter. It's all about moving data. In each case, we are concerned about the channels upon which that data travels—the highways our information rides along to get from place to place. When we take that information and put it on the Internet to move it we use the proverbial information superhighway.

The key question we need to ask ourselves is whether that highway is secure. Can anyone jump onto it and intercept the data we're moving? What about getting onto that highway to begin with? Just like a car uses an onramp to access a highway, you plug a cable into your

computer and that carries your information onto the Internet. And what about the destination. Once you get there (the cloud, SaaS) is our data safe there?

Think about how this all started — using a wireless to move the information from your computer to the Internet. But if we use that type of a wireless onramp to the information superhighway, we have security issues. The data becomes vulnerable once we transmit it through the air. By connecting to a wireless router we essentially open up a door to our computer and invite other people to come in and see whatever we have loaded onto our computers. The whole question of wireless access is also raised when we talk about cell phones and tablets. Those devices access the Internet and transmit information using unsecured networks as well.

Not only do we have issues of moving data (transmission), but we also have issues about situations where you move information to another place and leave it there- to store it. Cloud storage companies/websites end up storing the data on their own servers (in the "cloud"). Similarly, programs known as Software as a Service (SaaS) invoke all of the problems discussed because you are sending data to another company that is used in their programs, thus creating transmission issues, wireless problems and storage concerns. Not sure what "the cloud" is all about? The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility explained these technologies clearly when it stated:

> If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using "cloud computing." While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely "a fancy way of saying stuff's not on your computer."[1] From a more technical perspective, "cloud computing" encompasses several similar types of services under different names and brands, including: web-

---

[1] Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility Formal Opinion 2011-200, at 1, citing, Quinn Norton, "Byte Rights," Maximum PC, September 2010, at 12.

based e-mail, online data storage, software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), infrastructure-as-a-service("IaaS"), Amazon Elastic Cloud Compute ("Amazon EC2"), and Google Docs."[2]

Fast forward now to generative AI like Chat GPT. It's the same concern. Chat GPT becomes valuable when you use it to process your client's information. You ask it questions about your case so you can find some sort of answers — research, novel legal ideas, whatever. In order to get valuable answers, you need to give it specific information. That specific information is going to be client information. And once you move that client information to anywhere — the cloud, Chat GPT, whatever — the vulnerabilities of all of those technologies implicate the same ethical issues: the potential release or disclosure of confidential information (Rule 1.6), the potential loss of client information/property (a failure to safeguard client property per Rule 1.15), and the duty to supervise the vendors (Rule 5.3).

b. Yesterday's standard, applicable today.

It has long been established that lawyers could send unencrypted email regarding client matters, but that wasn't always the case. When the technology was first developed, the powers that be were opposed to permitting such email communication. However, things changed in the late 90s.

The ABA issued a formal opinion in 1999 which stated that there is a reasonable expectation of privacy despite the risk of interception and disclosure. The key development was that legislation was enacted making the interception of email a crime. In its Opinion, the ABA stated:

> "The Committee believes that e-mail communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy. The level of legal protection accorded e-mail transmissions, like that accorded other

[2] Pa Opinion 2011-200 at 1

> modes of electronic communication, also supports the reasonableness of an expectation of privacy for unencrypted e-mail transmissions. The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law. The Committee concludes, based upon current technology and law as we are informed of it, that a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a) in choosing that mode to communicate. This is principally because there is a reasonable expectation of privacy in its use."[3]

States, of course, followed suit and permitted the use of unencrypted email in the practice of law. What's key here is that we see the standard clearly— the reasonable expectation of privacy. It's important to understand the standard/rationale for permitting such email communications, because it continues to be relevant today. As new technologies are developed, the authorities apply the same reasoning. Consider the recent furor over gmail and other free email services.

In its Opinion 820, the New York State Bar Association opined about those free email systems.[4] The systems of yore were a concern because of the business model that the systems use to keep the service free. Here's how they worked: in return for providing the email service, "the provider's computers scan e-mails and send or display targeted advertising to the user of the service. The e-mail provider identifies the presumed interests of the service's user by scanning for keywords in e-mails opened by the user. The provider's computers then send advertising that reflects the keywords in the e-mail."[5] The obvious problem is that if a lawyer was using the email system for client work, then that lawyer was allowing the provider to scan confidential information.

---

[3] ABA Commission on Ethics and Professional Responsibility Formal Opinion 99-413

[4] New York State Bar Association Committee on Professional Ethics Opinion 820 – 2/8/08

[5] NYSBA Op. 820 at 2

When considering whether these new email systems would be permitted, the NY authorities first considered the rationale for permitting email back in the 90s. Email was allowed because, "there is a reasonable expectation that e-mails will be as private as other forms of telecommunication and…therefore…a lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information.[6] They applied that same reasoning to the question of free emails.

You'd think that the authorities would have banned the emails, given that their content was being read by the email system, right? Wrong. Even though the email messages in the system were scanned, the opinion noted that humans don't actually do the scanning. Rather, it's computers that take care of that task. Thus, they stated that "Merely scanning the content of e-mails by computer to generate computer advertising…does not pose a threat to client confidentiality, because the practice does not increase the risk of others obtaining knowledge of the e-mails or access to the e-mails' content."[7]

What the opinion is basically saying is that there continued to be a reasonable expectation of privacy in those email systems. Maybe the better way to phrase it is a reasonable expectation of "confidentiality," but the idea is the same (more on Rule 1.6, Confidentiality, later).

That ethical standard continued to be relevant and we saw it being applied later to a google product. On September 21, 2018 the Wall Street Journal reported that Google shares Gmail information with its app developers. But what's important is the type of information that's being shared and who viewed it. The WSJ article revealed that:

> Google Inc. told lawmakers it continues to allow other companies to scan and share data from Gmail accounts…the company allows app developers to scan Gmail accounts… outside app developers can access information about what products people buy, where

---

[6] NYSBA Op. 820 at 1

[7] NYSBA Op, 820 at 2

> they travel and which friends and colleagues they interact with the most. In some cases, employees at these app companies have read people's actual emails in order to improve their software algorithms.[8]

Did you get that last part? There are real human beings who are reading the contents of Gmail messages. What we know from NY Opinion 780 is that if human beings are reading the lawyer emails, then lawyers no longer have a reasonable expectation of privacy in Gmail.

Sure, we lack some specific data about which emails were read, but that doesn't change the conclusion. We might not know if lawyers' messages in particular were included in the messages that were scanned. But that's sort of exactly the problem — we don't know. And we don't have any way to control or restrict the app developers from reading anyone's emails, including our practice-related emails. Because of that reality I don't think that lawyers have a reasonable expectation of privacy in using Gmail any more. Our duty to protect client confidences set forth in Rule 1.6 precludes us from using the service. I'll tell you the truth, it actually looks like no one — lawyer nor otherwise — has a reasonable expectation of privacy with the platform. That's why I think lawyers need to stop using Gmail for practice related matters immediately.

The same standard is relevant today. When lawyers use generative AI like Chat GPT, we put our client information into the system. Open source systems which are trained on the internet at large take the information that's fed into it and use it in it's processing going forward. The Enterprise DNA blog explained that, "Chat GPT logs every conversation, including any personal data you share, and will use it as training data. Open AI's privacy policy states that the company collects personal information included in 'input, file uploads, or feedback' users provide to Chat GPT and its other services. The company's FAQ explicitly states that it will use

---

[8] https://www.wsj.com/articles/google-says-it-continues-to-allow-apps-to-scan-data-from-gmail-accounts-1537459989 last checked 7/3/2023.

your conversations to improve its AI language models and that your chats may be reviewed by human AI trainers."[9]

You can see how ye olde Email standard is still relevant. Lawyers do not have an expectation of privacy if we put our client information into generative AI programs alike Chat GPT. Similarly, we also happen to violate Rule 1.6…

c. Yesterday's standards, expanded and applicable in the future.

i. Confidentiality and the Cloud. The Reasonable Care Standard

The early decisions that addressed technology didn't always talk about "cloud computing" in particular, but they set the standard that would be followed when that technology arrived. Thus, the State of Nevada addressed the ability of lawyers to store confidential client information and/or communications in an electronic format on a server or other device that is not exclusively in the lawyer's control.[10] The Committee found that it was ethically permissible and stated that, "If the lawyer acts competently and reasonably to ensure the confidentiality of the information, then he or she does not violate [the rules] by simply contracting with a third parity to store the information…"[11]

The Committee said that the duty to save files on third party servers is the same as the duty to safeguard files that are put into third party warehouses, so contracting for such storage is not a per se confidentiality violation.[12] The lawyer wasn't strictly liable for an ethics violation

---

[9] https://blog.enterprisedna.co/is-chat-gpt-safe/#:~:text=No%2C%20Chat%20GPT%20is%20not%20confidential.&text=The%20company%27s%20FAQ%20explicitly%20states,reviewed%20by%20human%20AI%20trainers last checked July 2, 2023.

[10] State Bar of Nevada, Standing Committee on Ethics and Professional Responsibility,Formal Opinion No. 33, February 9, 2006, at 1.

[11] Nevada Opinion No. 33, at 1.

[12] Nevada Opinion No. 33, at 1.

"even if an unauthorized or inadvertent disclosure should occur".[13] Instead, the question was whether they exercised proper care. They articulated a standard that would be repeated in many following opinions when they said, "The lawyer must act competently and reasonably to safeguard confidential client information and communications from inadvertent and unauthorized disclosure."[14]

Similarly, New Jersey evaluated a technologically related issue— whether a lawyer can scan client files to a PDF, then archive them electronically and store those documents on the web.[15] Just like in Nevada, the concern was that Rule 1.6 requires "that the attorney 'exercise reasonable care' against the possibility of unauthorized access to client information."[16] The New Jersey Committee echoed the Nevada findings and stated that,

> "Reasonable Care…does not mean that "the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access…What the term 'reasonable care' means in a particular context is not capable of sweeping characterizations or broad pronouncements." at 3.

Given the changing nature of technology, the New Jersey Committee was reluctant to make a particularly bold decision but they did provide some elaboration of what constituted "reasonable care." They stated that,

> '"The Touchstone in using 'reasonable care' against unauthorized disclosure is that: (1) the lawyer has entrusted such documents to an outside provider in circumstances in which there is an enforceable obligation to preserve confidentiality and security, and (2) use is made of available technology to guard against reasonably foreseeable attempts to infiltrate the data. If the lawyer has come to the prudent professional judgment he has satisfied both these criteria, then 'reasonable care' will have been exercised." at 5

---

[13] Nevada Opinion No. 33, at 1.

[14] Nevada Opinion No. 33, at 1.

[15] State Bar of New Jersey, Supreme Court Advisory Committee on Professional Ethics, Opinion 701, April 10, 2006, 15 N.J.L. 897 April 24, 2006, at 2

[16] NJ Opinion 701, at 3.

That phrase, “reasonably foreseeable” was an indication of things to come. In fact, the standard evolved in a decision out of Maine. Maine agreed that the lawyer needs to take reasonable steps to protect confidentiality but they went further and they stated that,

> “the lawyer would be well-advised to include a contract provision requiring the contractor to inform the lawyer in the event the contractor becomes aware of any inappropriate use or disclosure of the confidential information. *The lawyer can then take steps to mitigate the consequences and can determine whether the underlying arrangement can be continued safely.* (emphasis added). at 2

This is the first time we see an extended affirmative duty on the lawyer’s part. Maine set forth the idea that the lawyer’s duty is ongoing and that there may be a time where a lawyer needs to actually take some action to protect the client information.

Arizona reviewed a question that was analogous to cloud storage and added a further elaboration of what it meant to be exercising reasonable care. Arizona said that if you’re going to use online storage sites, Competence (Rule 1.1) demands that you understand them. Specifically they stated that “the competence requirements…apply not only to a lawyer’s legal skills, but also generally to ‘those matters reasonably necessary for the representation..’ Therefore, as a prerequisite to making a determination regarding the reasonableness of online file security precautions, the lawyer must have, or consult someone with, competence in the field of online computer security.”[17] In other words, in order to show that you’re exercising reasonable care, you need to understand the systems or associate yourself with someone who has that understanding.

And there’s something more— here we see a further expansion of the affirmative duty. Not only must we take reasonable precautions to protect confidentiality and security of client information, but, the committee acknowledged that as technology changes, certain protective

---

[17] State Bar of Arizona, Opinion 09-04, 12/2009, at 1.

measures might become obsolete.[18] Thus, the Committee warned that "As technology advances occur, lawyers should periodically review security measures in place to ensure that they still reasonably protect the security and confidentiality of the clients' documents and information."[19] Thus, there is a continuing obligation to revisit the reasonability of the security that our vendors are utilizing. In other words, we can't take the "stick our heads in the sand approach".

A year later, the State of Alabama agreed and stated that,

> "Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third-party provider. If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider."[20]

In the same year, the New York Bar Association elaborated on that idea. In Opinion 842 they evaluated whether a lawyer could use an online data storage system to store and back up client confidential information. Like the other states that opined on the topic, they answered in the affirmative, subject to the same confidentiality concerns. They also confirmed the ongoing nature of the lawyer's duty if one were to make use of these systems. They stated:

> "10. Technology and the security of stored data are changing rapidly. Even after taking some or all of these steps (or similar steps), therefore, the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology. If the lawyer learns information suggesting that the security measures used by the online data storage provider are insufficient to adequately protect the confidentiality of client information, or if the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated. See Rule 1.4 (mandating

---

[18] Arizona Opinion 09-04 at 2.

[19] Arizona Opinion 09-04 at 1-2.

[20] Alabama Ethics Opinion 2010-02 at 16

communication with clients); see also N.Y. State 820 (2008) (addressing Web-based email services)."[21]

In the following, far less earth-shattering paragraph, the New York authorities also noted the need for lawyers to stay abreast of the law regarding technology. "Not only technology itself but also the law relating to technology and the protection of confidential communications is changing rapidly. Lawyers using online storage systems (and electronic means of communication generally) should monitor these legal developments, especially regarding instances when using technology may waive an otherwise applicable privilege. *[citation omitted]*."[22]

Do I even need to make the connection to Chat GPT? When you use that system, you give them your client information. It's the functional equivalent of storing it with them. Thus, all of the ethical standards that govern cloud computing apply to Chat GPT as well. That's why I say that not much has changed. The same holds true for Rule 1.15…

ii. Our Fiduciary Duty Under 1.15

In North Carolina we see an opinion that reveals the second of the two major ethical concerns with using cloud-based systems/software. That's the need to protect our client's information with the care required of a fiduciary as set forth in Rule 1.15.

Most people hear the Rule number "1.15" and think about trust accounts. It's true that the rule is most often invoked in our discussion about our client's money, but the rule actually has broader implications. Rule 1.15 governs our responsibilities with our client's property and money is just one type of client property that we might hold. Another type of property is the client's file.

---

[21] New York State Bar Association Opinion 842 (9/10.10) at 4.

[22] New York State Bar Association Opinion 842 (9/10.10) at 4.

The hard copy of your client's file is the client's property and we also know that Rule 1.15 mandates that we take steps to safeguard that property. When you think about it, however, the digital version of your client's file is also their property—you're simply holding it in computerized form. Any information about your client matter is part of their "file." Thus, if we release that to another individual (like a cloud storage vendor, or a generative AI program) we need to make sure that we're taking steps to safeguard that client property appropriately. That invokes Rule 1.15, which is why the North Carolina opinion states, "Rule 1.15 requires a lawyer to preserve client property, including information in a client's file such as client documents and lawyer work product, from risk of loss due to destruction, degradation, or loss. See also RPC 209 (noting the "general fiduciary duty to safeguard the property of a client")."[23]

In the end, the North Carolina authorities didn't provide any new ethical ideas, rather they simply confirmed that using SaaS (cloud computing), in particular, was not a violation. Specifically, they stated, "Lawyers can use SaaS, "provided steps are taken effectively to minimize the risk of inadvertent or unauthorized disclosure of confidential client information and to protect client property, including the information in a client's file, form risk of loss." But when you apply that to programs like Chat GPT you have a problem. When you give client information to those types of programs you have no way to "minimize the risk of inadvertent or unauthorized disclosure of confidential client information." Zero. There is no way to minimize the risk. In fact, you have to assume that the information will be spit out somewhere else at some time because the system told you that's a possibility.

Let's address something here — there are some systems that purport to give you an option to "opt out" of sharing your client data. Some systems might give us the option to simply "disallow" the collection and/or dissemination of that data. If lawyers actually did opt out, then

---

[23] The North Carolina State Bar, 2011 Formal Ethics Opinion 6, Issued in January 27, 2012.

that might change the calculation. But there are two problems with that. (1) trusting the tech companies to honor that pledge and (2) forgetting to end the collection/dissemination altogether.

Regarding the first, you'll have to forgive me for not trusting big tech, but consider the following excerpt from the website The Verge in their article, "Amazon confirms it holds on to Alexa data even if you delete audio files being used' by Makena Kelly and Nick Statt:

> Amazon has admitted that it doesn't always delete the stored data that it obtains through voice interactions with the company's Alexa and Echo devices — even after a user chooses to wipe the audio files from their account. The revelations, outlined explicitly by Amazon in a letter to Sen. Chris Coons (D-DE), which was published today and dated June 28th, sheds even more light on the company's privacy practices with regard to its digital voice assistant.[24]

Regarding the second — forgetting to deny/end the collection and dissemination of that information — it's really just a question of lawyers not having that heightened sense of awareness I'm always talking about.

We are inundated with requests to share information. Every device/program we use asks us if we can share data and we simply click "yes" oftentimes without even thinking. The constant barrage of such requests is likely desensitizing us to the dangers of granting those request. At some point we're going to end up sharing data for a device or system that is going to provide out client data to someone who shouldn't be seeing it.

iii. The Extension of our Duty to Supervise.

The day-to-day realities of the practice reveal that lawyers are not the only individuals in the office about whom we must be concerned when we decide to use technology. The commentary to Rule 1.6 confirms that: "[16]…A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client

---

[24] https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy, last checked 1/14/2022.

or who are subject to the lawyer's supervision." Various states have expanded upon that concept and discussed our larger responsibility to train our non-lawyer staff.

In an opinion we discussed earlier, the Maine Committee confirmed that the primary responsibility for confidentiality remains with the lawyer, but they also noted that the Maine rule "implies that lawyers have the responsibility to train, monitor, and discipline their non-lawyer staff in such a manner as to guard effectively against breaches of confidentiality. Failure to take steps to provide adequate training, to monitor performance, and to apply discipline for the purposes of enforcing adherence to ethical standards is grounds for concluding that the lawyer has violated [the rule]."[25]

Plus, our duties extend beyond keeping an eye on our in-house nonlawyer staff. The foundation for that was laid before the technology era when the Oregon State Bar addressed whether a lawyer could use a recycling service to dispose of client documents. The issue was whether doing so violated the rule on confidentiality because you would be exposing confidential client information to the recycling vendor. The opinion held that, "as long as Law Firm makes reasonable efforts to ensure that the recycling company's conduct is compatible with Law Firm's obligation to protect client information," using the service is permissible.[26] They further stated that "reasonable efforts include, at least, instructing the recycling company about Law Firms duties pursuant to Oregon RPC 1.6 and obtaining its agreement to treat all materials appropriately."[27] This is exactly the sentiment set forth by other bars regarding cloud computing vendors.

The Maine Committee noted that the technology vendor needs to be supervised as well. While the lawyer doesn't directly train or monitor the service provider employees, "the lawyer

---

[25] Maine Board of Overseers of the Bar, Opinion #194, Issued June 30, 2008, at 1-2.

[26] Oregon State Bar, Formal Opinion No. 2005-141, August 2005, at 386

[27] Oregon Opinion 2005-141 at 386.

retains the obligation to ensure that appropriate standards concerning client confidentiality are maintained by the contractor."[28]

The Oregon and Maine opinions marked the beginning of a trend, about which all lawyers must be aware. Over the past several decades we've seen states expand upon the duty for lawyers to be responsible for non-lawyers who are working for the firm, but not necessarily inside the firm's office. This was further exhibited in North Carolina's Formal Ethics Opinion 6, in which they stated,

> "Although a lawyer may use nonlawyers outside of the firm to assist in rendering legal services to clients, Rule 5.3(a) requires the lawyer to make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer. The extent of this obligation when using a SaaS vendor to store and manipulate confidential client information will depend upon the experience, stability, and reputation of the vendor. Given the rapidity with which computer technology changes, law firms are encouraged to consult periodically with professionals competent in the area of online security."[29]

New Hampshire went a little further and let us know that we can't pass the buck when it comes to the tech vendors. They made is clear that the duties of confidentiality and competence are ongoing and not delegable:[30]

> "When engaging a cloud computing provider or an intermediary who engages such a provider, the responsibility rests with the lawyer to ensure that the work is performed in a manner consistent with the lawyer's professional duties. Rule 5.3 (a). Additionally, under Rule 2.1, a lawyer must exercise independent professional judgment in representing a client and cannot hide behind a hired intermediary and ignore how client information is stored in or transmitted through the cloud.[31]

A short while ago, the ABA chimed in on the topic. In a batch of amendments, the ABA made a change to two letters in the title of Rule 5.3-- that's right, I said two letters in the *title* --

---

[28] Maine Board of Overseers of the Bar, Opinion #194, Issued June 30, 2008, at 2.

[29] North Carolina's 2011 Formal Ethics Opinion 6

[30] New Hampshire Opinion 2012-13/4, at 4.

[31] New Hampshire Opinion 2012-13/4, at 3.

and that change has profound implications. Rule 5.3 used to be called, "Responsibilities Regarding Nonlawyer Assistants." However, how it's called, "Responsibilities Regarding Nonlawyer Assistance." Did you catch that? The last two letters of the final word-- "Assistants" is now "Assistance." This is a big deal because it reflects a growing trend in the world of ethics. Yes, we are responsible for supervising our own staff, but today that duty extends to other parties like those that we would have once called "independent contractors." Anyone that we use in assistance, like vendors, are parties that we now have a duty to supervise. We get further guidance in this regard from new Comments [3] and [4] in Rule 5.3.

What we notice from those comments is that this change was brought about mostly because (a) lawyers now outsource many of the tasks that used to be completed in house and (b) there is an increased reliance on cloud storage and other technology-related vendors. Thus, the comments tell us that we must supervise nonlawyers outside the firm that we use for investigations, document management, cloud storage, etc., and the Comment also provides factors that should be considered when determining the extent of our obligations in these circumstances.

The new technologies that are powered by AI are no different from a supervision standpoint. We simply can not delegate our ability to supervise those technologies simply because we have vendors who assist us in utilizing them. All of the opinions regarding the lawyer's duty of supervision apply to these new technologies as well.

iv. The Emerging Affirmative Duty to Understand, Anticipate, and Act

I've tried to take the information that's been provided by the various state opinions and distill it down to some workable direction to attorneys. Here's how it looks to me:

All of these opinions make clear is that we need to be competent and protect client confidentiality. In order to do that we need to understand the technological systems, understand the security precautions that the vendors use, supervise the vendors appropriately, ensure that

the terms of service are adequate, and remember that the review of all of the foregoing is a continuing duty (plus some other stuff, but those are the biggies).

What's clear is that the opinions have created a significant affirmative duty for lawyers who choose to use cloud systems. *We have an ongoing obligation to understand, anticipate, and act.* We must understand the technology, the security, and the law. We must be able to anticipate security issues, problems presented by our nonlawyer staff, confidentiality concerns, and everything else. And if the situation requires it, we must act. We may be forced to change vendors, for instance, if we think our client's information is vulnerable. We may need to demand that vendor change some protocol. It could be anything.

The point is that we can't sit idly by. Ignorance is not bliss, it's an ethical violation. If we are going to utilize these systems we need to continually stay up to date on all relevant variables. It's an active, ongoing process.

2. Chatbots: the legal marketing device that could get you in trouble

Chatbots are used in legal marketing to help lawyers find valuable clients. The technology is basically a computer program that is powered by artificial intelligence and it simulates conversation with people. Potential clients who visit a firm's site can type questions and comments into a chatbox and, when doing so, they think they are speaking with a real person (or at least it's supposed to seem that way). Meanwhile, the bot collects contact info as well as other information about the potential client's case, analyzes it, and gives that info to the lawyer. The chatbot companies say that their AI allows them to sift out the tire kickers, identify the valuable prospects, and improve conversion rates from visitors to actual clients.

The chatbots are provided by tech vendors. A lawyer contracts with a vendor that offers the chatbot software, the vendor provides a bit of code that is inserted into the lawyer's website, and the chatbot becomes a part of the lawyer's site. Someone coming to the website

wouldn't know that another vendor is operating it— it simply looks like a chat box that is part of the lawyer's website.

Using a chatbot isn't necessarily a problem. What you need to be concerned about is the nature of the exchange between the bot and the potential client. Of course, it's a problem if a chat bot engages in conversation with a potential client and dispenses legal advice. But that's not likely to happen because that's not what the bots do. They are just supposed to be weeding out the garbage contacts from the good prospects. But in order to do that, the chatbot needs to ask the prospect some questions, and evaluate the data. That is where the problem could arise…

There is a conversation that goes on between the bot and the prospect. During that conversation the prospect will be providing information about their case. What we need to worry about is the potential that people who visit the lawyer's site and engage in a conversation with the chatbot end up being considered "prospective clients" under Rule 1.18. If they do attain that status, the lawyer could have conflict problems. To see what I mean, first understand how the rule works.

a. <u>How Rule 1.18 Works</u>

Rule 1.18 says that if a person "consults with a lawyer about the possibility of forming a client-lawyer relationship" they could be a prospective client. All they need to do is *consult* about the *possibility* of forming the lawyer client relationship. But what does that mean? Why should a lawyer care if someone is technically considered a "prospective client?"

First, you can't tell anyone about the information that the prospective client gave you. Rule 1.18(b) explains that "Even when no client-lawyer relationship ensues, a lawyer who has learned information from a prospective client shall not use or reveal that information…" Second, you might be conflicted out of representing people in the future. Even if you don't take the prospective client and never work on their matter, subsection (c) says that if you received information from the prospective client that could be significantly harmful to that person, and some time in the future a person approaches you to represent that new person against the

prospective client in the same matter, you might not be permitted to so so. You would be conflicted out of the representation.

That could be devastating. Think about it— if you have a consultation with someone about a lucrative matter and you decide not to take their case…but later you are approached by someone who wants you to represent them in that very case you can't take that other client. You could be forced to forego a lot of money in fees.

b. <u>The problem with chatbots</u>

So back to the bots and Rule 1.18. What's important is the trigger for becoming a prospective client, and as you saw from the rule above, the trigger is a consultation. The key question, of course, is, when does something rise to the level of a *consultation?* The answer is that it depends on the circumstances. But, in my opinion, the key circumstances to focus on are (1) what your website says and (2) the level of detail in the chatbot's communications.

If your website just lists your contact information you're going to be okay. If you simply put your information out there and someone sends you information about a case, that's not going create a prospective client relationship. Comment [2] confirms that: "…a consultation does not occur if a person provides information to a lawyer in response to advertising that merely describes the lawyer's education, experience, areas of practice, and contact information, or provides legal information of general interest." Basically, that comment is saying that if you simply tell someone that you exist and that you are qualified, it's not a "consultation." If someone replies in that situation, the person "communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship." That person, therefore, is not a prospective client.

However, you're going to have a problem if your website encourages people to offer information and your chatbot follows up by asking for information. The comment explains that "…a consultation is likely to have occurred if a lawyer…through the lawyer's advertising in any medium, specifically requests or invites the submission of information about a potential

representation without clear and reasonably understandable warnings and cautionary statements that limit the lawyer's obligations, and a person provides information in response."

If your site specifically requests or invites a person to submit information about a potential representation, and your chat bot provides information in response, then you are risking the creation of a prospective client relationship. Obviously, the ethical danger is dependent upon the responsiveness of the chatbot because the rule says that you have to "provide information in response." Well, the more lengthy, intense, and detailed the chatbot's responses, the more likely there will be a problem.

Oh, and don't get hung up on the fact that your chatbot is not a "person" under the rules. Personally, if the bot provides information I think a tribunal will see the software as an extension of the lawyer. Plus, if the AI software is doing its job correctly, the potential client should believe that they are actually communicating with a real person. For those reasons, I wouldn't be surprised if a tribunal concluded that the AI in the chatbot is the functional equivalent of a "person" for the purposes of the rule.

Of course, there is a huge get-out-of-trouble card. All you have to do is include the disclaimers set forth in the rule. If your site has "clear and reasonably understandable warnings and cautionary statements that limit the lawyer's obligations" as stated in Comment [2], you're probably ok. This, however, is a situation where you can win the ethical battle, but lose the overall war. What I mean by that is…what if this issue isn't raised in an ethics grievance? What if it is, instead, raised in a disqualification motion?

c. <u>Win the ethical battle, but lost the disqualification war</u>

Let's say you're in a medium sized firm that handles a variety of different types of matters. Your firm represents Business X and you've been their counsel on various issues for years. Your firm has a website that utilizes a chatbot to evaluate the strength of clients. You have language on the website that properly disclaims Rule 1.18. Someone visits your site and explains that they have a workplace discrimination claim. They provide details of the case to the chatbot. The bot inquiries further and the prospect provides more information, in fact, the

client wants to make sure that the lawyer with whom they are chatting has a complete understanding of the case (maybe they don't know it isn't a computer) so they provide a lot of details.

The chatbot sends the info to the attorney at the firm responsible for reviewing the contacts made by the chatbot and that lawyer thinks that the prospect has a great case. After reviewing the information, the attorney contacts the prospect and learns that the adverse party is Business X. However, the lawyer figures that the firm will probably be representing Business X in that matter because the firm does all of their work. As a result the firm doesn't take the potential client.

The prospect finds another lawyer, and they file suit against Business X. As the lawyer anticipated, the firm is representing Business X. The prospect's lawyer files a motion to disqualify you as counsel and you oppose it. You claim that there is no violation of the rule— the prospect never became a "prospective client" under Rule 1.18 because you had the proper disclaimer. And you're probably right. But there is a good chance that a judge will disqualify you anyway.

Remember, the judge isn't deciding discipline — the judge is deciding whether you should be disqualified. They don't necessarily care about the technicalities of the rules, they care about two things — the two things that are at the core of *every* conflict— loyalty and confidential information.

The critical question that the judge will ask was, *during the interaction the firm had with the prospect, did you learn confidential information from the other party?* And when the judge realizes that your chatbot gathered information that would ordinarily be considered confidential information and it was passed on to the lawyer in your firm for review, they're going to say you have a conflict and kick you out of the case. You're not going to be saved by the disclaimers because those disclaimers only helped you avoid discipline under Rule 1.18. In the disqualification context the court cares about loyalty and confidential information. And when it

finds out that you were privy to a slew of details from the potential client's case, they will disqualify you.

d. How to make chatbots safer

All of this doesn't mean that chatbots can't be used, they just need to be used carefully. What can you do to make the chatbot safer? Here are 5 ideas:

(1) Use disclaimers
(2) Make sure the bot is just gathering information and not giving any information. And if it does give information, make sure it's super limited. Keep Comment [4] to Rule 1.18 in mind which states, "In order to avoid acquiring disqualifying information from a prospective client, a lawyer considering whether or not to undertake a new matter should limit the initial consultation to only such information as reasonably appears necessary for that purpose."
(3) Go over Rule 1.18 with the vendor supplying your chatbot. Make sure they understand it. also explain the disqualification issue. Remember, most tech vendors have no idea about the details rules like 1.18.
(4) Train the staff/lawyers in your office who are responsible for following up on the leads developed by the bot. Let them know about Rule 1.18 and the issue of disqualification.
(5) Create a process that limits the exposure the lawyers who review the information provided by the chatbots. It is possible to screen those attorneys per 1.18(d)(2). Here's what that section states, in part:

> (d) When the lawyer has received disqualifying information… representation is permissible if…(2) the lawyer who received the information took reasonable measures to avoid exposure to more disqualifying information than was reasonably necessary to determine whether to represent the prospective client; and (i) the disqualified lawyer is timely screened from any participation in the matter and is apportioned no part of the fee therefrom; and (ii) written notice is promptly given to the prospective client.

3. Attorney ethics in the meta verse.

The future is the metaverse. At least, that's what Facebook thinks. I mean, they changed their name to Meta in anticipation of the growth of that part of the internet. Since it appears to be a large part of life in the not-to-distant future, Rule 1.1 (Competence) demands that we understand what it is and the ethical implications that are posed to lawyers.

What is the metaverse? It's basically an alternate reality that exists on line. I gathered a few excerpts from some reputable online sources to explain the metaverse:

> *According to a Fast Company article, Dan Eckert, managing director, AI and emerging technology, PwC explained:*
>
> > An extended reality metaverse is still 3-5 years out: The metaverse—or should we say metaverses—has been around since the time of multiplayer computer games and even Second Life/AOL/Compuserve.
> > Yes, plural–there will not be just one–there will be many, each designed for focused communities, capabilities, and experiences. The Metaverse, as being shouted by everyone, is not shipping (yet), but we are starting to see the building blocks released every day.[32]
>
> *Bernard Marr explained in Forbes:*
>
> > Digitization, datafication and virtualization
> >
> > During 2020 and 2021, many of us experienced the virtualization of our offices and workplaces, as remote working arrangements were swiftly put in place. This was just a crisis-driven surge of a much longer-term trend. In 2022, we will become increasingly familiar with the concept of a "metaverse" – persistent digital worlds that exist in parallel with the physical world we live in. Inside these metaverses – such as the one proposed recently by Facebook founder Mark Zuckerberg – we will carry out many of the functions we're used to doing in the real world, including working, playing, and socializing. As the rate of digitization increases, these metaverses will model and simulate the real world with growing accuracy, allowing us to have more immersive, convincing, and ultimately valuable experiences within the digital realm. While many of us have experienced somewhat immersive virtual realities through headsets, a range of new devices coming to the market will soon greatly improve the experience offering tactile feedback and even smells. Ericsson, which provided VR headsets to employees working from home during the pandemic, and is developing what it calls an "internet of senses," has predicted that by 2030 virtual experiences will be available that will be indistinguishable from reality. That might be looking a little

[32] https://www.fastcompany.com/90704618/the-biggest-tech-trends-of-2022, last checked 1/12/2022.

> further ahead than we are interested in for this article. But, along with a new Matrix movie, 2022 will undoubtedly take us a step closer to entering the matrix for ourselves.[33]

Finally, from a CNBC article - "Investors are paying millions for virtual land in the metaverse" by Chris DiLella and Andrea Day:

> It's no secret the real estate market is skyrocketing, but the Covid pandemic is creating another little-known land rush. Indeed, some investors are paying millions for plots of land — not in New York or Beverly Hills. In fact, the plots do not physically exist here on Earth.
>
> Rather, the land is located online, in a set of virtual worlds that tech insiders have dubbed the metaverse. Prices for plots have soared as much as 500% in the last few months ever since Facebook announced it was going all-in on virtual reality, even changing its corporate name to Meta Platforms.
>
> "The metaverse is the next iteration of social media," said Andrew Kiguel, CEO of Toronto-based Tokens.com, which invests in metaverse real estate and non fungible token-related digital assets.[34]

The connection to attorney ethics goes beyond merely the need to be competent and understand the concept. It can also apply to our actions when we use the meta verse ourselves. Lawyers will surely participate, in a professional and personal capacity. I could envision lawyers having a virtual presence of some sort in the metaverse, I must admit that I don't know how that would look, but I'm sure it's going to happen. In addition, lawyers will participate in the metaverse in ways that were unrelated to the practice of law. The thing to remember is that no matter what type of presence we have in the metaverse, the ethics rules will still apply to your behavior.

Your behavior in the metaverse is going to be regulated by the disciplinary system in the real world. Any action you take as a practicing lawyer that occurs in the metaverse will be governed by the rules of attorney ethics. And it doesn't stop there. Even actions that are not related to the practice could be covered by the rules. If you steal something in the metaverse,

---

[33] https://www.forbes.com/sites/bernardmarr/2021/09/27/the-5-biggest-technology-trends-in-2022/?sh=4bafc07c2414, last checked 1/12/2022.

[34] https://www.cnbc.com/2022/01/12/investors-are-paying-millions-for-virtual-land-in-the-metaverse.html, last checked 1/17/2022.

you'll need to answer to Rule 8.4(b): "It is professional misconduct for a lawyer to (b) commit a criminal act that reflects adversely on the lawyers honesty, trustworthiness, or fitness as a lawyer in other respects." This isn't an alien concept- we all know that our personal behavior is within the purview of the ethics authorities. This is simply another part of our personal life, and we need to be aware that the long arm of the disciplinary system reaches into alternate universes as well as the real world.

Here's an interesting quirk that might arise in the metaverse. What if you assume an alternate personality. I'm going to guess that a lot of people who participate in the metaverse will become a character that's different from their true persona. It's just speculation on my part, but I have to believe that there are a lot of people who are looking forward to the metaverse as a way to escape from the life that they currently lead. But lawyers need to beware. Taking on an alternate identity could end up somehow violating Rule 8.4(c) — "It is professional misconduct for a lawyer to: (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation…"

4. More controversial uses of AI technology and the role lawyers should (?) play.

Let's consider some of the more controversial uses of the technology: predictive policing,[35], biases in algorithms[36] and surveillance uses like facial recognition[37].

a. Predictive Policing

One hot use for AI technology is called, "predictive policing" Nature.com explained,

> …police agencies hope to 'do more with less' by outsourcing their evaluations of crime data to analytics and technology companies that produce 'predictive policing' systems. These use algorithms to forecast where crimes are likely to occur and who might commit them, and to make recommendations for allocating police resources. Despite wide adoption, predictive policing is still in its infancy, open to bias and hard to evaluate.
>
> Predictive models tie crimes to people or places. Offender-based modelling creates risk profiles for individuals in the criminal justice system on the basis of age, criminal record, employment history and social affiliations. Police departments, judges or parole boards use these profiles — such as estimates of how likely a person is to be involved in a shooting — to decide whether the individual should be incarcerated, referred to social services or put under surveillance. Geospatial modelling generates risk profiles for locations. Jurisdictions are divided into grid cells (each typically around 50 square metres), and algorithms that have been trained using crime and environmental data predict where and when officers should patrol to detect or deter crime.[38]

It doesn't take much to understand how this sort of programming could end up yielding discriminatory results. The very word "predictive" in the name of the technology gives an indication of the problem.

b. Biases in Algorithms

The final article from Nature.com that I'm going to quote today addresses the ethics issue with biases in algorithms. In an article entitled, "Bias detectives: the researchers striving to make algorithms fair", the website explained the concern that arises when AI algorithms are used to help…and how that could go awry.

---

[35] https://www.nature.com/articles/541458a, last checked 6/19/2021.

[36] https://www.nature.com/articles/d41586-018-05469-3, last checked 6/19/2021.

[37] https://www.nature.com/articles/d41586-019-03775-y, last checked 6/19/2021.

[38] https://www.nature.com/articles/541458a, last checked 6/20/2021.

> In 2015, a worried father asked Rhema Vaithianathan a question that still weighs on her mind. A small crowd had gathered in a basement room in Pittsburgh, Pennsylvania, to hear her explain how software might tackle child abuse. Each day, the area's hotline receives dozens of calls from people who suspect that a child is in danger; some of these are then flagged by call-centre staff for investigation. But the system does not catch all cases of abuse. Vaithianathan and her colleagues had just won a half-million-dollar contract to build an algorithm to help.
>
> Vaithianathan, a health economist who co-directs the Centre for Social Data Analytics at the Auckland University of Technology in New Zealand, told the crowd how the algorithm might work. For example, a tool trained on reams of data — including family backgrounds and criminal records — could generate risk scores when calls come in. That could help call screeners to flag which families to investigate.
>
> After Vaithianathan invited questions from her audience, the father stood up to speak. He had struggled with drug addiction, he said, and social workers had removed a child from his home in the past. But he had been clean for some time. With a computer assessing his records, would the effort he'd made to turn his life around count for nothing? In other words: would algorithms judge him unfairly?

c. The dangerous rise of the surveillance state

If you're not aware of the ever-growing encroachment of the surveillance state, then you must live under a rock. But don't worry…no matter how well you're hidden under that boulder, they know where you are. Who are "they?"

QIUET — WE ASK THE QUESTIONS!!

All kidding aside, the concern about the surveillance state is no longer the thing of conspiracy theories. I'm not some aluminum-foil-hat-wearing eccentric. Rather, I'm a teacher who likes to watch how paradigms shift. And any review of credible news resources today reveals that we are in the midst of an important paradigm shift. The use of artificially intelligent surveillance technologies has expanded significantly, and those resources are becoming a primary part of the governmental toolkit across the globe. It's time for lawyers to start to consider all of this, and to think about what, if any, obligation we have as a practice.

A quick Google search reveals the extent to which people are being watched by the government these days. We saw surveillance technology employed during the COVID lockdowns. The Wall Street Journal reported about the experience of a man in Beijing: "Late one

night recently, he received an automated phone call from Beijing authorities saying he had been in proximity to someone with a confirmed Covid infection, which means he can't go to public places until the health code on his phone turns green. That could involve two PCR tests and several days' wait."[39]

The use of technology to monitor people is certainly not limited to our devices. In an article entitled, "Chinese 'gait recognition' tech IDs people by how they walk " Dake Kang of the Associated Press reported:

> Chinese authorities have begun deploying a new surveillance tool: "gait recognition" software that uses people's body shapes and how they walk to identify them, even when their faces are hidden from cameras.
>
> Already used by police on the streets of Beijing and Shanghai, "gait recognition" is part of a push across China to develop artificial-intelligence and data-driven surveillance that is raising concern about how far the technology will go.[40]

Facial recognition technology is apparently being used in relatively nefarious ways in society today. In Nature.com authors Richard Van Noorden & Davide Castelvecchi wrote an article in 2019 entitled. "Science publishers review ethics of research on Chinese minority groups":

> Two science publishers are reviewing the ethics of research papers in which scientists backed by China's government used DNA or facial-recognition technology to study minority groups in the country, such as the predominantly Muslim Uyghur population.
>
> Springer Nature (which publishes Nature) and Wiley want to check that the study participants gave informed consent, after researchers and journalists raised concerns that the papers were connected to China's heavy surveillance operations in the northwestern province of Xinjiang. China has attracted widespread international condemnation — and US sanctions — for mass detentions and other human-rights violations in the province. The Chinese government says that it is conducting a re-education campaign in the region to quell what it calls a terrorist movement.

---

[39] China's Lockdowns Prompt a Rethinking of Life Plans Among the Young by Liyan Qi and Shen Lu, May 29, 2022, https://www.wsj.com/articles/chinas-lockdowns-prompt-a-rethinking-of-life-plans-among-the-young-11653822000 last checked 7/8/2022.

[40] https://apnews.com/article/china-technology-beijing-business-international-news-bf75dd1c26c947b7826d270a16e2658a last checked 7/7/2022.

> ‘We are very concerned about research which involves consent from vulnerable populations…’[41]

The use of this technology is by no means restricted to China. Quite the contrary, it’s already being put into use across the globe. The MIT Technology Review explained how France is making great efforts to disseminate monitoring technology:

> Since 2015, the year of the Bataclan terrorist attacks, the number of cameras in Paris has increased fourfold. The police have used such cameras to enforce pandemic lockdown measures and monitor protests like those of the Gilets Jaunes. And a new nationwide security law, adopted last year, allows for video surveillance by police drones during events like protests and marches.[42]

The technology has even expanded to the evaluation of DNA. NPR interviewed Yves Moreau, an engineer and professor at the Catholic University in Leuven, Belgium, and they discussed the use of DNA data in surveillance. They acknowledged that “DNA data has been used to track and identify alleged criminals for decades,”[43] But the concern is:

> [The technology] has been rolled out on a very large scale. And what we have seen is that this technology is being rolled out in particular in the west of China. And in 2016, 2017, blood samples from essentially the entire population, people 12 to 65 in Xinjiang, was collected and potentially put in that database. And it can be part of a broader system of what we call total surveillance.[44]

The use of technology in this way made the professor concerned about its relationship to historical acts of genocide:

> I’m extremely concerned about this because in history, actually, if you look back in the first half of the 20th century, German and then Belgian colonists in Rwanda and Burundi actually went there, and they were using pseudoscientific ideas about race and assigned

---

[41] https://www.nature.com/articles/d41586-019-03775-y, last checked 1/17/2022.

[42] MIT Technology Review, “Marseille’s battle against the surveillance state” by Fleur Macdonald, June 13, 2022, https://www.technologyreview.com/2022/06/13/1053650/marseille-fight-surveillance-state/ last checked 7/8/2022.

[43] https://www.npr.org/2019/12/07/785804791/uighurs-and-genetic-surveillance-in-china last checked 7/8/2022.

[44] https://www.npr.org/2019/12/07/785804791/uighurs-and-genetic-surveillance-in-china last checked 7/8/2022.

people to a particular ethnicity. That actually was a significant factor in genocides. And the risk for this in the midterm is actually really worrying.[45]

The paradox is that there are good uses for the technology.

In Fortune magazine, author Jeremy Kahn evaluated whether Artificial Intelligence could be used to prevent future mass shootings. While the author was skeptical it could work, he could not rule the possible benefits of using AI in this context. He explained that one option is to "use computer vision algorithms to try to detect people attempting to carry weapons on to school grounds. There are already a number of A.I. software and CCTV camera vendors that claim to offer 'gun detection' algorithms."[46] Another possible use of AI technology is "to create "smart guns" that are fitted with cameras and A.I. software. Such a system could be set to detect whether the person being aimed at is a child and prevent the gun from being fired."[47] He also noted that "it is possible that this kind of A.I. could help flag troubled individuals who are at risk of committing violence."[48]

In the article, Mr Kahn acknowledges that there are serious questions about the practical effectiveness of these systems. But that's not really relevant for our discussion in this program. My purpose for bringing these ideas up is not to debate the efficacy of these systems, rather, it's to point out that the existence of AI motoring capabilities is not a problem, per se. There are certainly a huge number of potential societal benefits of the technology.

---

[45] https://www.npr.org/2019/12/07/785804791/uighurs-and-genetic-surveillance-in-china last checked 7/8/2022.

[46] "After Uvalde: Could A.I. prevent another school shooting?" By Jeremy Kahn, May 31, 2022, https://fortune.com/2022/05/31/ai-prevent-uvalde-mass-school-shooting/ last checked 7/8/2022.

[47] "After Uvalde: Could A.I. prevent another school shooting?" By Jeremy Kahn, May 31, 2022, https://fortune.com/2022/05/31/ai-prevent-uvalde-mass-school-shooting/ last checked 7/8/2022.

[48] "After Uvalde: Could A.I. prevent another school shooting?" By Jeremy Kahn, May 31, 2022, https://fortune.com/2022/05/31/ai-prevent-uvalde-mass-school-shooting/ last checked 7/8/2022.

Using the AI powered technology for beneficial purposes — like tracking domestic terrorists, for example — is something few people would probably oppose. The problem is that once you give the government the authority to use the technology in tracking bad guys, you let them employ that technology whenever they thing they're going after bad guys. And they get to determine who the "bad guys" are. Wired magazine reported on research by the Surveillance Technology Oversight Project ("STOP"). Their conclusion: "A surveillance state built to track certain types of behavior can easily, and inevitably, be adapted to other ends."[49]

The potential for misuse of this technology is enormous. It's not just the generic, philosophical concern about the intrusion on civil liberties. The concern is that it will be used for improper political purposes: to stifle dissent, monitor people with views that question the current authorities, etc. And the concern isn't really about any particular side of the political spectrum. It's about whomever might be in power. You know the old adage — power corrupts, absolute power corrupts absolutely. Unfortunately, both sides of the political aisle have that potential.

d. Some people are taking action

1. Private Groups

Now you can see what makes this issue so difficult. If put in the right hands, this technology could help society. But if it's abused, it could be quite harmful. For that reason I'd never argue that the use of this technology should be eliminated, but that it should be monitored and controlled. And there are plenty of groups trying to address the situation. Take, for instance,

> Nano, a 39-year-old developer, wants to make residents of Marseille more aware that they are being watched. She is part of a group called Technopolice that has been organizing efforts to map the rise of video surveillance. With some 1,600 cameras in the city, there is plenty to find. Mixed in among them, Nano says, are 50 smart cameras

[49] "The Surveillance State Is Primed for Criminalized Abortion," by Lily May Newman, May, 2022. https://www.wired.com/story/surveillance-police-roe-v-wade-abortion/ last checked 7/8/2022.

> designed to detect and flag up suspicious behavior, though she is unsure where they are or how they are being used.[50]

2. Governments

It's become clear that there needs to be some larger restriction on this type of AI.

Bernard Marr explained in Forbes:

> Governments, too, clearly understand that there is a need for a regulatory framework, as evidenced by the existence of the EU's proposed Artificial Intelligence Act. The proposed act prohibits authorities from using AI to create social scoring systems, as well as from using facial recognition tools in public places.[51]

Various researchers have been raising their voices about the concerns with the technologies and it appears that, "governments are trying to make software more accountable."[52]

> Last December, the New York City Council passed a bill to set up a task force that will recommend how to publicly share information about algorithms and investigate them for bias. This year, France's president, Emmanuel Macron, has said that the country will make all algorithms used by its government open. And in guidance issued this month, the UK government called for those working with data in the public sector to be transparent and accountable. Europe's General Data Protection Regulation (GDPR), which came into force at the end of May, is also expected to promote algorithmic accountability.[53]

3. The Tech World

For their part, the AI world seems to be catching on. A recent article explained that, "Ethicists have long debated the impacts of AI and sought ways to use the technology for good, such as in health care. But researchers are now realizing that they need to embed ethics into the formulation of their research and understand the potential harms of algorithmic injustice…"[54]

---

[50] MIT Technology Review, "Marseille's battle against the surveillance state" by Fleur Macdonald, June 13, 2022, https://www.technologyreview.com/2022/06/13/1053650/marseille-fight-surveillance-state/ last checked 7/8/2022.

[51] https://www.forbes.com/sites/bernardmarr/2021/09/27/the-5-biggest-technology-trends-in-2022/?sh=4bafc07c2414, last checked 1/12/2022.

[52] https://www.nature.com/articles/d41586-018-05469-3, last checked 6/20/2021.

[53] https://www.nature.com/articles/d41586-018-05469-3, last checked 6/20/2021.

[54] https://www.nature.com/articles/d41586-020-00160-y, last checked 6/19/2021.

4. Lawyers?

I believe there is a role for lawyers in this fight as well. And I think the ethics rules demand that we fill it.

i. Lawyers have always had a responsibility to larger societal issues. Consider Pro Bono Work.

The lawyer's duty to help the poor has been long established. Actually, it's not just the "poor" because the category also includes the "disadvantaged" and the "underserved." What the issue is really about is helping people obtain access to justice. The category thus includes those people who have a barrier to access to justice and usually that barrier is a financial one. This obligation has been accepted in the practice for some time now.

We see a reference to this duty as far back as 1965 in the now outdated disciplinary rules, the Model Code of Professional Responsibility (that *Code* was eventually scrapped in its entirety and our existing disciplinary rules are based on the Model *Rules* of Professional Responsibility which were promulgated by the ABA in 1983). The Code stated, "As a society increases in size, sophistication and technology, the body of laws which is required to control that society also increases in size, scope and complexity. With this growth, the law directly affects more and more facets of individual behavior, creating an expanding need for legal services on the part of the individual members of the society."[55] In other words, as society advances, the obstacles to access to justice increase. That only enhances the need for lawyers to help the disadvantaged. Over the years, scholars have expanded upon that idea.

Professor Deborah L. Rhode (now of Stanford Law School) set forth a variety of justifications for the pro bono duty in an article she wrote back in 1999 in the Fordham Law Review. She explained that, "Lawyers have a monopoly on legal services, thus creating the

---

[55] See the Model Code footnote to EC 2-25, citing Comment, Providing Legal Services for the Middle Class in Civil Matters: The Problem, the Duty and a Solution, 26 U. PITT. L REV. 811, 811-12 (1965).

duty to help provide them for the poor."[56] Additionally, lawyers are a key guardian of justice and for that reason we have the obligation to provide legal services for those who can't afford them. Professor Rhode pointed to a more practical justification as well: "the benefit that such work confers upon the lawyers themselves," which includes the, "intrinsic satisfactions that accompany public service."[57] She continued, "The primary rationale for pro bono contributions rests on two premises: first, that access to legal services is a fundamental need, and second, that lawyers have some responsibility to help make those services available. The first claim is widely acknowledged."[58] Proof that it continues to be is widely acknowledged comes from the State of New York where recently Chief Judge Jonathan Lippman of the New York Court of Appeals acknowledged that "lawyers have a professional responsibility to promote greater access to justice."[59] He explained that, "as far back as judges and lawyers have existed, the pursuit of equal justice for all, rich and poor alike, has been the hallmark of our profession." And the responsibility doesn't stop with practicing attorneys. He continued, "each attorney has an obligation to foster the values of justice, equality, and the rule of law, and it is imperative that law students gain a recognition of this obligation as part of their legal training." [60]

The idea that lawyers should "give back" to society isn't so controversial. In fact, my gut tells me that the majority of people in the practice would agree with the need for lawyers to help

---

[56] Deborah L. Rhode, Cultures of Commitment: Pro Bono for Lawyers and Law Students, 67 Fordham L. Rev. 2415 (1999) at 2419.

[57] Deborah L. Rhode, Cultures of Commitment: Pro Bono for Lawyers and Law Students, 67 Fordham L. Rev. 2415 (1999) at 2420.

[58] Deborah L. Rhode, Cultures of Commitment: Pro Bono for Lawyers and Law Students, 67 Fordham L. Rev. 2415 (1999) at 2418.

[59] http://www.nycourts.gov/attorneys/probono/FAQsBarAdmission.pdf, last checked by the author on 12/27/2014.

[60] http://www.nycourts.gov/attorneys/probono/FAQsBarAdmission.pdf, last checked by the author on 12/27/2014.

the disadvantaged community. In theory, it seems to simply be an extension of our otherwise accepted societal wide notion of helping the needy.

ii. The Preamble as justification for lawyers taking action

Lawyers have a large role in society. We don't just owe a duty to our clients, rather the codes of professionalism in every state acknowledge that we also owe a duty to our communities and even society as a whole. That's why we champion things like Access to Justice, Diversity and Inclusion, and other similarly important ideals. It's because we know that our special role allows us to have an oversized impact in realizing those concepts. Plus, the privilege that we have to practice law demands that we take responsibility for making such important paradigms become a reality. I believe that the same obligation exists with AI powered facial recognition technology.

The ethics rules reflect the requirement for lawyers to pursue these larger goals. For instance, in the Preamble to the Rules, we find the following section:

> Preamble [1] A lawyer, as a member of the legal profession, is a representative of clients, an officer of the legal system and a public citizen having special responsibility for the quality of justice.

What does it mean to have a "special responsibility?" The very nature of the word "special" means that it's something out of the ordinary. When read in connection with the rest of the section, I believe that the special responsibility includes ensuring that the "quality of justice" is in step with societal advancements.

For instance, there was a time when our practice was made up of almost all white men. But as society advanced, we grew to appreciate the importance of diversity. In fact, the practice eventually made diversity a goal and today we have a significant emphasis on that — including, in some states, MCLE that's geared toward elimination of bias. That requirement is an example of how we took our "special responsibility for the quality of justice," made changes in the

practice and brought about a desired change. Today we have an opportunity to do that again, in an even bigger way. And example of the latest evolution in thinking is the idea of "access to justice."

As I mentioned earlier, the idea of ensuring that more people have access to justice is not a new concept. What is new, however, is the emphasis. It's only been the past several years that you've heard people talking about this concept in a more vocal manner. In fact, we see a reference in the rules:

> Preamble [6] …A lawyer should be mindful of deficiencies in the administration of justice and of the fact that the poor, and sometimes persons who are not poor, cannot afford adequate legal assistance. Therefore, all lawyers should devote professional time and resources and use civic influence to ensure equal access to our system of justice for all those who because of economic or social barriers cannot afford or secure adequate legal counsel. A lawyer should aid the legal profession in pursuing these objectives and should help the bar regulate itself in the public interest.

If lawyers actually pursue the mandate of the rules— if we devote time and resources to ensure equal access to our justice system for all, then we could make wide reaching societal change. That change affects people beyond the practice because it's a society-wide effort. By reducing these obstacles to justice, lawyers have a real chance to save the world.

It makes me wonder — should lawyers be talking a larger role in monitoring artificial intelligence throughout society? I mean, beyond considering the disciplinary implications. I'm talking about a larger role throughout society. It seems that our ethics rules mandate that we take a larger role. Look at the Preamble again, except now consider the issue of AI:

> [1] A lawyer, as a member of the legal profession, is a representative of clients, an officer of the legal system and a public citizen having special responsibility for the quality of justice.
>
> [5] A lawyer's conduct should conform to the requirements of the law, both in professional service to clients and in the lawyer's business and personal affairs. A lawyer should use the law's procedures only for legitimate purposes and not to harass or intimidate others. A lawyer should demonstrate respect for the legal system and for those who serve it, including judges, other lawyers and public officials. While it is a lawyer's duty, when necessary, to challenge the rectitude of official action, it is also a lawyer's duty to uphold legal process.

> [6] As a public citizen, a lawyer should seek improvement of the law, access to the legal system, the administration of justice and the quality of service rendered by the legal profession. As a member of a learned profession, a lawyer should cultivate knowledge of the law beyond its use for clients, employ that knowledge in reform of the law and work to strengthen legal education.

It appears that AI powered surveillance like facial recognition technology is being used to take advantage of vulnerable people. When one combines the other dangerous uses of artificial intelligence, then very serious concern for society as a whole. Maybe it's time for lawyers to add this issue to the roster of societal issues that we, as a profession confront. The need to do so seems to stem quite clearly from the obligations set forth above from the Preamble.

South Carolina Bar
Continuing Legal Education Division

2024 SC BAR CONVENTION

Technology

Saturday, January 20

The Bits and Bytes of Cryptocurrency Litigation

Graham L. Newman

358 So.3d 24
District Court of Appeal of Florida, Fourth District.

Daniela Souto COE, Appellant,
v.
Reinier Nicolaas RAUTENBERG, Appellee.

No. 4D22-510
|
[February 15, 2023]

Synopsis

Background: Wife filed petition for dissolution of marriage against husband. Wife later filed motion for contempt and past due child support based on husband's failure to comply with temporary child support order and was awarded past due child support. The Circuit Court, 15th Judicial Circuit, Palm Beach County, Scott Kerner, J., entered final judgment of dissolution, which established timesharing schedule, awarded wife past due child support, distributed marital property, and ordered payment of ongoing child support. Wife appealed.

Holdings: The District Court of Appeal, Damoorgian, J., held that:

trial court erred in failing to set holiday and school break timesharing schedule;

trial court improperly diminished wife's equitable distribution of cryptocurrency asset by deducting award to wife on her motion for past due child support from original amount of marital cryptocurrency and then dividing the remaining amount in half;

trial court erred in not requiring husband to reimburse wife for half the cost of recovering hard drive containing marital cryptocurrency;

trial court was required to make ruling on wife's motion for child support retroactive to date when parties did not reside together in the same household; and

trial court erred in ordering wife to pay $402.80 per month in child support for both children without stating the amount of child support that would be owed for youngest child after eldest child was no longer entitled to receive support.

Affirmed in part, reversed in part, and remanded.

Procedural Posture(s): On Appeal; Request for Retroactive Award of Child Support; Petition for Contempt for Failure to Pay Child Support; Petition for Divorce or Dissolution.

***25** Appeal from the Circuit Court for the Fifteenth Judicial Circuit, Palm Beach County; Scott R. Kerner, Judge; L.T. Case No. 50-2017-DR-002714-XXXX-SB.

Attorneys and Law Firms

Nancy A. Hass of Nancy A. Hass, P.A., Fort Lauderdale, for appellant.

No appearance for appellee.

Opinion

Damoorgian, J.

Daniela Souto Coe ("Former Wife") appeals the final judgment dissolving her marriage to Reinier Nicolaas Rautenberg ("Former Husband"). On appeal, Former Wife argues the trial court erred in: (1) ordering a bi-weekly rotating timesharing schedule; (2) declining to set a holiday or school break schedule; (3) distributing the marital Bitcoin assets and liabilities; (4) failing to properly address Former Wife's pending motions; and (5) awarding child support without making certain findings. We affirm on the first issue without further comment. For the reasons discussed below, we reverse on the remaining issues.

The parties were married in 2005 and have two children. Former Wife filed a petition for dissolution of marriage in March 2017, requesting therein an award of child support "retroactive to the date when the parties last resided together or the last 24 months prior to the filing of the Petition for Dissolution of Marriage." The petition also requested the trial court equitably distribute the parties' marital assets which, at the time, primarily consisted of 10 Bitcoins.

***26** During the pendency of the dissolution proceedings, the trial court entered an agreed order for temporary relief requiring Former Husband to pay $720 per month in temporary child support. The agreed order also provided as follows regarding retroactive child support: "The parties agree to the retroactive period of January 2016 through December 2017, and that the amount of retroactive child

support ... due from Husband to Wife during this period is reserved until further agreement of the parties or Court order."

Former Husband did not comply with the temporary child support order, prompting Former Wife to file a motion for contempt and for past due child support. Following a hearing, the trial court entered an agreed order awarding Former Wife $12,704.07 in past due child support for the period of January 1, 2018, through December 31, 2019. The agreed order also allowed Former Wife to "convert the equivalent portion of marital Bitcoins in her possession ... as the Husband's payment of the past due child support." At that time, $12,704.07 was the equivalent of 1.2 Bitcoins.

The matter was ultimately set for a final hearing. Prior to the final hearing, Former Wife filed several motions, three of which are relevant to this appeal. First, Former Wife moved for child support retroactive to the date when the parties no longer resided together in the same household. Second, Former Wife moved for past due child support for the period of January 2020 through November 2021. Third, Former Wife moved for reimbursement of the $1,851.20 she spent to recover the Bitcoin asset. [1]

The matter proceeded to a final hearing as scheduled, with both parties appearing pro se. At the beginning of the hearing, the trial court advised the parties "we're going to start off with [Former Wife's] motions" and asked that the parties "save your objections for your response." Consistent with her motions, Former Wife requested past due child support for "2020 and 2021" as well as retroactive child support for the "two years prior" to the filing of the petition for dissolution of marriage. After hearing argument from Former Husband, the trial court asked Former Wife if she had "any final word on your motion," to which Former Wife reiterated her position that she was seeking retroactive support "from the date of filing to two years, which is what the statute allows." The trial court then stated it would take the issue under advisement, and proceeded to address the equitable distribution and timesharing issues.

As to equitable distribution of the Bitcoin asset, the parties agreed the marital estate originally consisted of 10 Bitcoins. Both parties also agreed that Former Husband's original share of the asset (5 Bitcoins) had since been reduced by 1.2 Bitcoins (as payment for past due child support), thus leaving Former Husband with 3.8 Bitcoins as his equitable share of the asset. Former Wife also requested, consistent with her motion, that Former Husband reimburse her half of the cost to recover the Bitcoin hard drive. Notably, Former Husband told the trial court "[i]t was never an issue" when asked if he had "an objection to paying half the cost."

Following the hearing, the trial court entered a final judgment of dissolution of marriage wherein it did the following. First, the trial court ordered a bi-weekly rotating timesharing schedule. With the ***27** exception of Mother's Day and Father's Day, the trial court declined to set a holiday or school break timesharing schedule. Instead, the final judgment provided as follows: "Requests to alter this schedule may be temporarily accomplished by the parties only through a prior written agreement of the party seeking to temporarily modify the alternating schedule."

Second, the trial court awarded Former Wife $22,954.75 in past due child support for the period of December 31, 2019, through February 1, 2022. The final judgment did not address Former Wife's motion for child support retroactive to the date when the parties no longer resided together in the same household.

Third, the trial court equitably distributed the Bitcoin asset as follows:

> The [parties] both testified that their marital estate assets originally consisted of 10 marital Bitcoins ....
>
> ....
>
> The 1.2 Bitcoins listed by the Wife as a non-marital asset will remain a non-marital asset of the Wife. The remaining 8.8 Bitcoins are determined to be marital property, each party initially entitled to 4.4 Bitcoins. However, before distribution to the Husband, the [Wife] is entitled to a set-off [of] $22,954.75, before the distribution of the 4.4 bitcoins from the [Wife] to the [Husband].

The final judgment did not mention Former Husband reimbursing Former Wife for half the cost of recovering the Bitcoin hard drive.

Finally, the trial court ordered Former Wife to pay child support in the amount of $402.80 per month for both children. Neither the final judgment nor the child support guidelines worksheet attached thereto stated the amount of child support that would be owed for the youngest child after the eldest child was no longer entitled to receive support.

The standard of review regarding equitable distribution, timesharing, and child support is abuse of discretion. *See O'Neill v. O'Neill*, 305 So. 3d 551, 553–54 (Fla. 4th DCA 2020) (equitable distribution and child support); *Krift v. Obenour*, 152 So. 3d 645, 647 (Fla. 4th DCA 2014) (timesharing). To the extent Former Wife argues the trial court violated her right to due process, we apply the *de novo* standard. *Dobson v. U.S. Bank Nat'l Ass'n*, 217 So. 3d 1173, 1174 (Fla. 5th DCA 2017).

Former Wife first argues the trial court erred in failing to set a holiday and school break timesharing schedule. We agree. Despite recognizing at the hearing that the parties had an acrimonious parenting relationship, the trial court declined to set a holiday or school break timesharing schedule in the final judgment. Instead, the trial court left the responsibility of setting such a schedule to the parties. This was error. *See Blackburn v. Blackburn*, 103 So. 3d 941, 942 (Fla. 2d DCA 2012) ("[T]he magistrate erroneously declined to set a holiday time-sharing schedule as requested. As a result, the parties who already have exhibited animosity toward one another are left with the responsibility of setting a schedule by which they can share time with the children on major holidays."); *Mills v. Johnson*, 147 So. 3d 1023, 1025 (Fla. 2d DCA 2014) ("In light of the fact that the magistrate determined that the parties have a 'contentious parenting relationship,' it seems particularly imperative for the magistrate to recommend a holiday time-sharing schedule."). We accordingly reverse on this issue and remand for the trial court to set a holiday and school break timesharing schedule.

Former Wife next argues the trial court miscalculated the number of marital ***28** Bitcoins that were subject to equitable distribution. Specifically, she argues that instead of deducting the 1.2 Bitcoins—previously awarded to Former Wife as payment for past due child support—from the original 10 marital Bitcoins and then equally distributing the remaining 8.8 Bitcoins, the trial court should have deducted the 1.2 Bitcoins from Former Husband's original share of 5 Bitcoins, thus leaving Former Husband with 3.8 Bitcoins, not 4.4 Bitcoins. Former Wife further argues the trial court erred in not requiring Former Husband to reimburse her for half the cost of recovering the Bitcoin hard drive. We agree.

By deducting the 1.2 Bitcoins from the original 10 marital Bitcoins and then dividing the remaining 8.8 Bitcoins, the trial court improperly diminished Former Wife's equitable distribution of the Bitcoin asset. This is because Former Wife had already been awarded the 1.2 Bitcoins from *Former Husband's* share of the asset as payment for past due child support. In other words, Former Husband's original marital share (5 Bitcoins) had already been reduced to 3.8 Bitcoins at the time of the final hearing. Therefore, the trial court should have awarded Former Wife her original share of the asset (5 Bitcoins) and Former Husband 3.8 Bitcoins. The trial court further erred in not requiring Former Husband to reimburse Former Wife for half the cost of recovering the Bitcoin hard drive, especially considering Former Husband agreed to reimbursing half of the cost at the final hearing. We accordingly reverse on this issue and remand with instructions that the trial court award Former Wife 5 Bitcoins and Former Husband 3.8 Bitcoins, and order Former Husband to reimburse Former Wife half of the cost of recovering the Bitcoin hard drive. Consistent with the final judgment, before distributing the 3.8 Bitcoins to Former Husband, the trial court shall award Former Wife the equivalent of $22,954.75 in Bitcoin from Former Husband's share of the asset as payment for past due child support.

Former Wife next argues that by asking the parties to refrain from objecting, the trial court "refus[ed] to permit the Wife to have each of her Motions heard, separately, and, fully," thereby violating her right to due process. This, in turn, also resulted in the trial court failing to rule on Former Wife's motion for retroactive child support. We disagree with Former Wife's due process violation argument. Nonetheless, the trial court should have ruled on Former Wife's motion for child support retroactive to the date when the parties did not reside together in the same household, especially considering the order for temporary relief reflects the parties agreed Former Husband owed retroactive child support for this period: "The parties agree to the retroactive period of January 2016 through December 2017, and that the amount of retroactive child support ... due from Husband to Wife during this period is reserved until further agreement of the parties or Court order." *See* § 61.30(17), Fla. Stat. (2022) ("In an initial determination of child support, ... the court has discretion to award child support retroactive to the date when the parents did not reside together in the same household with the child, not to exceed a period of 24 months preceding the filing of the petition, regardless of whether that date precedes the filing of the petition."). We accordingly reverse and remand for the trial court to determine the amount of retroactive child support due from Former Husband for the period of January 2016 through December 2017.

Former Wife lastly argues the trial court erred in ordering her to pay $402.80 per month in child support for both children

without stating, in either the final ***29** judgment or the child support guidelines worksheet, the amount of child support that will be owed for the youngest child after the eldest child is no longer entitled to receive support. We agree. *See* § 61.13(1)(a)1.b., Fla. Stat. (2022) ("All child support orders ... entered on or after October 1, 2010, *must* provide .... [a] schedule, based on the record existing at the time of the order, stating the amount of the monthly child support obligation for all the minor children at the time of the order *and the amount of child support that will be owed for any remaining children after one or more of the children are no longer entitled to receive child support* ...." (emphasis added)). We accordingly reverse on this issue and remand for the trial court to make the required finding.

Affirmed in part, reversed in part, and remanded.

Gross and Kuntz, JJ., concur.

All Citations

358 So.3d 24, 48 Fla. L. Weekly D353

Footnotes

1 The hard drive containing the Bitcoins was damaged at some point, and Former Wife hired a company to recover the data.

54 Cal.App.5th 25
Court of Appeal, First District, Division 3, California.

IN RE the MARRIAGE OF
Erica and Francis DESOUZA.
Erica DeSouza, Respondent,
v.
Francis DeSouza, Appellant.

A156311
|
Filed 8/10/2020

Synopsis

Background: In post-dissolution proceeding, former husband appealed from post-judgment order of the Superior Court, San Francisco County, No. FDI12778498, Richard C. Berra, J., finding he breached his fiduciary duty to his former wife, and ordering him to transfer cryptocurrency to her pursuant to the parties' judgment of dissolution and to pay her attorney fees and costs.

Holdings: The Court of Appeal, Siggins, Presiding Justice, held that:

trial court's finding that husband failed to disclose material information about his cryptocurrency investments was supported by substantial evidence, and

trial court's finding that husband's failure to disclose material information about his cryptocurrency investments caused impairment to wife's community interest was supported by substantial evidence.

Affirmed.

Procedural Posture(s): On Appeal; Judgment.

****891** Trial Court: San Francisco County, Trial Judge: Hon. Richard C. Berra (City & County of San Francisco Super. Ct. No. FDI12778498)

Attorneys and Law Firms

Philip S. Silvestry, Gregory R. Ellis for Appellant.

Samantha Bley DeJean, San Francisco, Juliana Yanez, Robert A. Olson, Los Angeles, Eleanor S. Ruth for Respondent.

Opinion

Siggins, P.J.

***27** Francis DeSouza appeals from a postjudgment order finding he breached his fiduciary duty to his former wife Erica and ordering him to transfer bitcoins and other cryptocurrency to her pursuant to the parties' judgment of dissolution and to pay her attorneys' fees and costs. [1] Francis argues he did not breach his fiduciary duty because information he ***28** withheld about his cryptocurrency investments was not material and, alternatively, there was no substantial evidence his breach impaired Erica's interest in their community estate. Neither point has merit. We affirm.

BACKGROUND

I. Francis Invests in Bitcoins

In January 2013 Erica served Francis with a petition for dissolution of marriage, along with an automatic temporary restraining order that, among other things, prohibited him from "[t]ransferring, encumbering, hypothecating, concealing, or in any way disposing of any property, real or personal, whether community, quasi-community, or separate, without the written consent of the other party or an order of the court, except in the usual course of business or for the necessities of life."

In April 2013, Francis initiated three bitcoin-related transactions. On April 9 or 10, he wired $45,000 to Mt. Gox Company Ltd. (Mt. Gox), a Japanese bitcoin exchange, to purchase bitcoins. Francis never received any bitcoins for this money, nor recovered the transferred funds.

****892** On April 10, 2013, Francis arranged for his friend and colleague Wences Casares to purchase 558.32 bitcoins from Mt. Gox for $99,451 on his behalf. Wences completed the purchase and transferred the bitcoins, along with an additional gift of five bitcoins (jointly, the Wences bitcoins), to Francis's digital wallet. [2]

On April 12, Francis had his associate Khaled Hassounah purchase an additional 498.89 bitcoins from Mt. Gox for $44,940 (the Khaled bitcoins) on his behalf. Khaled was to transfer these bitcoins from his own Mt. Gox account to

Francis's digital wallet. Although he bought the bitcoins as agreed, Khaled never completed the transfer and the 498.89 bitcoins remained with Mt. Gox.

In December 2013 and again in August 2014, Francis moved the Wences bitcoins from one digital wallet to another. In 2017 he learned that the Wences bitcoins had "forked," an automatic process that generates dividends from bitcoin holdings in the form of new currency, "bitcoin cash" and "bitcoin gold."

II. The Khaled Bitcoins Are Enmeshed in the Mt. Gox Bankruptcy

By April 2013, Mt. Gox was having regulatory difficulties with the U.S. government. On April 11 it briefly suspended trading. In June 2013 federal ***29** agents froze two bank accounts associated with the exchange and seized millions of dollars for its alleged failures to comply with federal regulations. Mt. Gox suspended withdrawals to be processed in U.S. dollars.

By late 2013 or early 2014, Mt. Gox lost hundreds of thousands of bitcoins to hacking, embezzlement, or both. Bitcoin expert Dr. Charles Evans testified for Erica that as early as March 2013, "anyone who was active on the Bitcoin discussion boards, anyone who was making an effort to get to know the Bitcoin community, knew that Mt. Gox was having trouble left, right, and sideways. [¶] And my personal opinion at the time was only an idiot would leave his Bitcoins on Mt. Gox." Dr. Evans reviewed e-mails between Francis, Khaled and Wences in the spring of 2013. One such e-mail from Wences to Francis advised him to "[b]uy your Bitcoins on Mt. Gox, then get the Bitcoins off and put them into Blockchain.info," and led Dr. Evans to conclude Francis was aware of the problems with Mt. Gox when he arranged his proxy purchases in April 2013. [3]

Francis discovered by December 2013 that he could not get the Khaled bitcoins ****893** out of Mt. Gox. In February 2014, Mt. Gox halted all withdrawals and filed for bankruptcy. By May 2014, Francis knew of the bankruptcy. He hoped the situation would get resolved but made no effort to recover the Khaled bitcoins or the initial $45,000 he wired to Mt. Gox, which were tied up in the bankruptcy. He testified, "[t]here wasn't much money when they went bankrupt, so at the point it wasn't worth chasing them for little money, and now there's nobody to chase." Eventually Khaled filed a proof of claim in bankruptcy for the 498.8 bitcoins, which were still in his name, on Francis's behalf.

***30** Francis filed his preliminary schedule of assets and debts in the divorce action in February 2014 and his final disclosure in July 2016. Both schedules disclosed his ownership of 1,062.21 bitcoins.

The parties' property issues were tried in February 2017. In September 2017 the court issued a final statement of decision, found the Wences and Khaled bitcoins to be community property and ordered them divided evenly in kind between the parties, along with any derivative cryptocurrency.

After entry of the dissolution judgment on December 8, 2017, Erica sought her half of the community bitcoins. Only then did Francis disclose that the Khaled bitcoins were tied up in the Mt. Gox bankruptcy. On December 18, 2017, the day after bitcoin's value hit a high of $19,783.06, Francis divulged that he possessed only 613.53 of the 1062.21 community bitcoins. In a December 22, 2017 e-mail to his attorney copied to Erica's counsel, Francis wrote that "[t]he exchange I was using to buy bitcoins, Mt. Gox, was hacked and then went bankrupt. I was able to take out 613.53 bitcoins." [4] Francis had also failed to inform Erica prior to the judgment that he used Wences and Khaled as proxies for his bitcoin purchases, that bitcoin cash and gold had been generated from the bitcoin investments, and that he transferred of cryptocurrency between digital wallets.

On December 31, 2017, the price of bitcoin was $13,500. The Khaled bitcoins had appreciated from their initial purchase price of approximately $45,000 to around $8 million.

III. Erica Seeks Postjudgment Relief

In January 2018 Erica moved for an emergency order compelling Francis to immediately transfer her full interest in community bitcoins to her and for remedies afforded by the Family Code for his failure to timely and adequately disclose information about the bitcoin investments. Following a January 12, 2018 hearing the court ordered Francis to immediately transfer to Erica half of the 613.53 bitcoins and associated bitcoin cash and gold he had in his possession, to show cause why he should not be ordered to transfer an additional 224.34 bitcoins and proportional cryptocurrency, and to pay Erica's attorney's fees and costs pursuant to Family Code sections 721 and 1100. It is undisputed that Francis

transferred 306.765 bitcoins to Erica in order to comply with the first part of the court's order.

Erica's request for the order was tried over four days between June and August 2018. On October 19 the court issued its final statement of decision ***31** finding that Francis committed a series of transgressions surrounding ****894** his purchase and handling of the bitcoins. The court found Francis violated the automatic restraining order and his fiduciary duties when, without Erica's knowledge or agreement, he sent $45,000 to Mt. Gox to purchase bitcoins, committed additional community funds so that Wences and Khaled could purchase bitcoins on his behalf, and moved the Wences bitcoins between bitcoin wallets. The court further found that while Francis possessed documentation of the proxy purchases since April 2013, he "not only refused to disclose, but affirmatively hid from [Erica] their involvement until February 9, 2018."

In addition to concealing his bitcoin purchases and use of proxies, Francis's failure to inform Erica about the Mt. Gox bankruptcy further breached his fiduciary duty. "This was a material fact he should have disclosed to [Erica]. Had he disclosed these important facts [Erica] would have had the ability to object to a division in kind of the bitcoins and/or protect her interest in the bitcoins by requesting the Court to use its equitable powers to protect her from [Francis's] decision to purchase the bitcoins as he did which tied up a substantial portion in bankruptcy." Francis again breached his fiduciary duty when he failed to list the $45,000 sent to Mt. Gox in either of his declarations of disclosure, failed to file a bankruptcy claim for those funds, withheld information about his bitcoin investments during discovery, failed to produce and falsely denied having documentation related to the bitcoins, and failed to disclose the cryptocurrency generated by forks.

The court ordered Francis to transfer $22,500 in cash and 249.445 additional bitcoins to Erica, along with the corresponding bitcoin gold and bitcoin cash. Francis was also ordered to pay Erica's attorneys' fees and costs incurred in bringing her motion.

Francis filed a timely appeal after the court denied his new trial motion.

DISCUSSION

I. Legal Principles

Family Code section 721[5] "recognizes the confidential relationship held by spouses. That relationship is a fiduciary relationship 'impos[ing] a ***32** duty of the highest good faith and fair dealing on each spouse.' [Citation.] Also within that division, section 1100 addresses management and control of community property. Subdivision (e) of section 1100 provides: 'Each spouse shall act with respect to the other spouse in the management and control of the community ****895** assets and liabilities in accordance with the general rules governing fiduciary relationships which control the actions of persons having relationships of personal confidence as specified in Section 721, until such time as the assets and liabilities have been divided by the parties or by a court. This duty includes the obligation to make full disclosure to the other spouse of all material facts and information regarding the existence, characterization, and valuation of all assets in which the community has or may have an interest and debts for which the community is or may be liable, and to provide equal access to all information, records, and books that pertain to the value and character of those assets and debts, upon request.' " (*In re Marriage of Schleich* (2017) 8 Cal.App.5th 267, 276-277, 213 Cal.Rptr.3d 665 (*Schleich*).)

This fiduciary duty continues after separation, including "[t]he accurate and complete disclosure of all assets and liabilities in which the party has or may have an interest or obligation and all current earnings, accumulations, and expenses, including an immediate, full, and accurate update or augmentation to the extent there have been material changes." (§ 2102, subd. (a)(1).) "Taken together, these Family Code provisions impose on a managing spouse affirmative, wide-ranging duties to disclose and account for the existence, valuation, and disposition of all community assets from the date of separation through final property division. These statutes obligate a managing spouse to disclose soon after separation all the property that belongs or might belong to the community, and its value, and then to account for the management of that property, revealing any material changes in the community estate, such as the transfer or loss of assets. This strict transparency both discourages unfair dealing and empowers the nonmanaging spouse to remedy any breach of fiduciary duty by giving that spouse the 'information concerning the [community's] business' needed for the exercise of his or her rights [citations], including

the right to pursue a claim for 'impairment to' his or her interest in ***33** the community estate [citation]." (*In re Marriage of Prentis-Margulis & Margulis* (2011) 198 Cal.App.4th 1252, 1270-1271, 130 Cal.Rptr.3d 327 italics omitted (*Margulis*).)

Section 1101 thus affords each spouse a claim against the other for any breach of fiduciary duty that results in an impairment to his or her interest in the community estate, "including, but not limited to, a single transaction or a pattern or series of transactions, which transaction or transactions have caused or will cause a detrimental impact" to the claimant spouse's interest in the community estate. (§ 1101, subd. (a).) Remedies for a breach of this duty that impairs another spouse's interest in the community estate include "an award to the other spouse of 50 percent, or an amount equal to 50 percent, of any asset undisclosed or transferred in breach of the fiduciary duty plus attorney's fees and court costs." (§ 1101, subd. (g); see *id*., subd. (a).)

Our courts have varied in stating the standard of review that applies when the trier of fact has found a breach of this duty. (See *In re Marriage of Kamgar* (2017) 18 Cal.App.5th 136, 144, 226 Cal.Rptr.3d 234 [substantial evidence]; *Schleich, supra,* 8 Cal.App.5th at pp. 283-284, 213 Cal.Rptr.3d 665 [abuse of discretion].) The difference in approach does not matter here. "The abuse of discretion standard is not a unified standard; the deference it calls for varies according to the aspect of a trial court's ruling under review. The trial court's findings of fact are reviewed for substantial evidence, its conclusions of law are reviewed de novo, and its application of the law to the facts is reversible only if arbitrary and capricious." (****896** *Haraguchi v. Superior Court* (2008) 43 Cal.4th 706, 711-712, 76 Cal.Rptr.3d 250, 182 P.3d 579.) " 'When a trial court's factual determination is attacked on the ground that there is no substantial evidence to sustain it, the power of an appellate court begins and ends with the determination as to whether, on the entire record, there is substantial evidence, contradicted or uncontradicted, which will support the determination, and when two or more inferences can reasonably be deduced from the facts, a reviewing court is without power to substitute its deductions for those of the trial court. If such substantial evidence be found, it is of no consequence that the trial court believing other evidence, or drawing other reasonable inferences, might have reached a contrary conclusion.' " (*In re Marriage of Goodwin-Mitchell & Mitchell* (2019) 40 Cal.App.5th 232, 238-239, 253 Cal.Rptr.3d 123.)

II. Materiality

As noted in *Schleich, supra,* 8 Cal.App.5th at pp. 276-277, 213 Cal.Rptr.3d 665, subdivision (e) of section 1100 requires each spouse to fully disclose all material facts regarding community assets. Francis argues his failure to fully inform Erica ***34** about the bitcoin investments was not "material" within the meaning of this provision because "no evidence suggested Erica's knowledge of this information would have affected her decision-making in the least." The court's contrary finding is supported by substantial evidence and within its discretion.

The court found the suspension and bankruptcy of Mt. Gox less than a year after Francis used community funds and proxies to purchase bitcoins from the exchange "substantially impaired [Erica's] undivided one-half interest in the community Bitcoin estate. She was unable to sell or transfer a substantial portion of her bitcoins. The purchase made by Wences was previously transferred to [Francis's] blockchain wallet but Khaled's purchase and the $45,000 deposit by [Francis] are subject to the bankruptcy and are inaccessible and if [Erica] were ever to receive some or all of her bitcoins or the cash it most likely will be at a significant loss, or even turn out to be worthless." The court further found that Francis's 2014 and 2015 declarations of disclosure listed the total amount of his bitcoin purchases, but failed to disclose that 498 of those 1062.21 bitcoins were (1) purchased by and still in Khaled's nominal possession; and (2) tied up in the Mt. Gox bankruptcy. These facts, the court found, were material. "Had he disclosed these important facts [Erica] would have had the ability to object to a division in kind of the [total] bitcoins and/or protect her interest in the bitcoins by requesting the Court use its equitable powers to protect her from [Francis's] unilateral decision to purchase the bitcoins."

Francis asserts the evidence that Erica generally took no interest in the couple's finances during or after their marriage proved that she would not have done anything to protect her interest in the bitcoin investments had he informed her about them. The trial court reasonably disagreed. Erica's lack of involvement or interest in the couple's finances before they separated is undisputed, but it sheds little if any light on what she would do to protect her financial interests after retaining divorce counsel, filing for divorce, and serving Francis with restraining orders that barred him from making unilateral decisions involving the community

estate. Even Francis acknowledges in his reply brief the "general validity" of Erica's point that "[a] spouse who may be reliant on and trusting of the other during marriage, may well exercise independent judgment and rely on new advisors after separation." Indeed.

****897** Nor did Francis's evidence compel the court to accept his view that Erica "continued her indifference to issues surrounding the community's investments" after the parties separated. His support for this characterization consists of his own conclusory testimony to that effect and one postseparation incident in which Erica agreed to his request to invest $50,000 of community funds in a friend's company. None of this, plainly, compels a finding that Erica would have done nothing throughout years of divorce litigation to ***35** preserve her interest in an investment that was worth millions of dollars by the time the property judgment issued.

Francis more specifically asserts that his failure to disclose his initial purchase of bitcoins is immaterial because "the court did not base its Family Code section 1101, subdivision (g) award on a finding that Francis had breached his fiduciary duty by failing to disclose his investment to Erica beforehand, or for that matter by keeping the Khaled bitcoins at Mt. Gox or by employing proxies to purchase bitcoins." Rather, he maintains, the findings of breach "[a]t most" "related to [his] failure to tell Erica at various times *well after* he purchased the bitcoins about his use of proxies and the Mt. Gox bankruptcy." Not so. The court expressly (and nonexclusively) found that Francis "breached his fiduciary duties to [Erica] *when he purchased the bitcoins in 2013*...." (Italics added.) And it found the Mt. Gox suspension and bankruptcy "substantially impaired" Erica's interest in the Khaled bitcoins by rendering them inaccessible and potentially worthless. "[T]hese facts were clearly 'material' information that should have been made known" to her. Francis's distortion of the court's express findings does not help him.

Neither does his suggestion he cannot be faulted for failing to disclose the Mt. Gox bankruptcy because, although he received a notice of bankruptcy in May 2014, he testified that he was unaware the Khaled bitcoins were caught up in it before Khaled told him in December 2017. The trial court expressly disbelieved this testimony. "Given the fact that Khaled testified that he worked with [Francis's] brother for a period of at least ten years and had not only socialized with Francis, but had traveled with him too, it is more likely than not that [Francis] knew of the loss of bitcoins to bankruptcy earlier than December 2017." We will not second-guess the court's credibility assessment. (*Thompson v. Asimos* (2016) 6 Cal.App.5th 970, 981, 212 Cal.Rptr.3d 158.)

The court's finding that Francis failed to disclose material information about his bitcoin investments is supported by substantial evidence and within its broad discretion.

III. Impairment

Francis argues that, even if he failed to disclose material information, his disclosure caused no impairment to Erica's community interest because, even with the Khaled bitcoins tied up in the Mt. Gox bankruptcy, the Wences bitcoins "earned millions of dollars for the community, thereby greatly ***36** enriching, not impairing, the community estate." Again, the trial court reasonably disagreed. True, the bitcoins Wences purchased for Francis and moved out of Mt. Gox before the bankruptcy grew from an initial value of roughly $100,000 to around $3.45 million by August 2018.[6] But the financial success of one ****898** undisclosed investment does not erase the harm to the community estate, and Erica, occasioned by a separate undisclosed transaction.

In re Marriage of Feldman (2007) 153 Cal.App.4th 1470, 1483, 64 Cal.Rptr.3d 29 is instructive. There, a husband contended his failure to include a $1 million bond in his financial disclosures in violation of section 2102, subdivision (a)(1) was excused by his failure to include the corresponding debt he incurred to finance the bond's purchase. The contention was unavailing. As the appellate court observed, "[t]he statutory policy in favor of disclosure contains no exception for debts and assets that offset each other, and [husband] has cited no authority to support such a position." (*Feldman*, at p. 1483.) So too here. Francis attempts to distinguish *Feldman* on the ground it addresses sanctions for failures to comply with financial disclosure obligations under section 2102 rather than spousal liability for fiduciary breaches more generally, but the distinction is immaterial. As observed in *Margulis, supra,* 198 Cal.App.4th at p. 1270, 130 Cal.Rptr.3d 327, section 2102, together with sections 721, 1100 and 1101, is part of the integrated statutory scheme that implements the policy of fiduciary care by imposing "wide-ranging duties to disclose and account for the existence, valuation, and disposition of all community assets from the date of separation through final division." (*Margulis*, at pp. 1270–1271, italics omitted.)

The statutory policy at issue in *Feldman*, therefore, is equally compelling here. Alternatively, Francis insists the Khaled and Wences bitcoins were merely two facets of one unitary investment and, therefore, he cannot be penalized for one and not credited for the other. But the trial reasonably court drew a different inference from the evidence, so we will not disturb it.

Lastly, Francis's contention that his nondisclosures did not *cause* the bankruptcy and resulting devaluation of the Khaled bitcoins largely rests on and reiterates his argument that the nondisclosures were immaterial. Accordingly, it fails for the same reasons. In any event, nothing in the trial court's order suggests its findings are premised on such an unlikely surmise.

***37 DISPOSITION**

The order is affirmed.

Fujisaki, J., and Petrou, J., concurred.

All Citations

54 Cal.App.5th 25, 266 Cal.Rptr.3d 890, 20 Cal. Daily Op. Serv. 9144, 2020 Daily Journal D.A.R. 9518

Footnotes

1 For clarity, we adopt the parties' practice of identifying themselves and other key actors by their first names. We intend no disrespect by this practice.

2 A digital wallet is a secure storage method that can only be accessed by the holder of a private key.

3 In his written report, Dr. Evans elaborated that "Hack #I took place beginning as far back as 2011 through the time that MtGOX ceased operation. According to MtGOX CEO, Mark Karpeles, hackers siphoned off approximately 750,000 bitcoins held in reserve for customer accounts along with 100,000 of MtGOX's own bitcoins. This amounted to between 6% and 7% of the total number of all the bitcoins in circulation at that time, worth approximately $7.25 billion at current prices as of the date of this report.

"Whether Hack # I indeed was a hack, in the sense of an external breach, or it was an 'inside job', remains the subject of speculation among persons who are interested in the MtGOX saga. Relevant here is not whether the theft was committed by external or internal actors, but that it was widely recognized that MtGOX was an accidental success, and its founder and chief executive was in over his head, as evidenced by email from Wences Casares to Francis DeSouza dated 22 March 2013, in which Casares instructed DeSouza, 'To buy bitcoin open an account at mtgox.com ... To store and use bitcoins open an account at blockchain.info. ... [¶]• Hack #2 took place in March 2014, concurrent with MtGOX's bankruptcy filing. In this instance, the hackers released a file called MtGox2014Leak.zip that they claimed was a database of MtGOX transaction records, with users' personal data intentionally removed.' "

4 Apparently a "forking" event in August 2017 added 50.205 bitcoins to the bitcoins Wences purchased for Francis, resulting in the 613.53 figure he reported in December 2017.

5 With exceptions not relevant here, subdivision (b) of Family Code, section 721 provides that "in transactions between themselves, spouses are subject to the general rules governing fiduciary relationships that control the actions of persons occupying confidential relations with each other. This confidential relationship imposes a duty of the highest good faith and fair dealing on each spouse, and neither shall take any unfair advantage of the other. This confidential relationship is a fiduciary relationship subject to the same rights and duties of

nonmarital business partners, as provided in Sections 16403, 16404, and 16503 of the Corporations Code, including, but not limited to, the following:

> "(1) Providing each spouse access at all times to any books kept regarding a transaction for the purposes of inspection and copying. [¶] (2) Rendering upon request, true and full information of all things affecting any transaction that concerns the community property. Nothing in this section is intended to impose a duty for either spouse to keep detailed books and records of community property transactions. [¶] (3) Accounting to the spouse, and holding as a trustee, any benefit or profit derived from any transaction by one spouse without the consent of the other spouse that concerns the community property."

Further statutory citations are to the Family Code.

6 Francis does not dispute his liability to the community for the initial $45,000 wired to Mt. Gox.

533 F.Supp.3d 1321
United States District Court,
N.D. Georgia, Atlanta Division.

Mary SHEA, Plaintiff,
v.
BEST BUY HOMES, LLC and
Mike Cherwenka, Defendants.

CIVIL ACTION FILE NO. 1:20-CV-02387-SCJ
|
Signed 03/30/2021

Synopsis

Background: Vendor of residential real property brought an action against prospective purchaser for fraud, negligent misrepresentation, promissory estoppel, and violations of the Georgia Uniform Securities Act of 2008 (GUSA) and Georgia Racketeer Influenced and Corrupt Organizations Act (RICO) arising out of a purchase and sale agreement in which prospective purchaser offered to buy vendor's house at the list price of $125,000 with 30% of the purchase price to be paid with a form of cryptocurrency and sought a declaratory judgment that the agreement was illegal and void. Prospective purchaser moved to dismiss for failure to state a claim.

Holdings: The District Court, Steve C. Jones, J., held that:

purchase and sale agreement was void for illegality;

merger clause in purchase and sale agreement was unenforceable;

vendor alleged plausible sale of investment contract that was neither registered nor exempt, supporting claim for violation of GUSA;

vendor alleged plausible pattern of racketeering activity as required to state RICO claim;

vendor's allegations did not support a claim for fraud;

vendor's allegations did not support a claim for negligent misrepresentation; and

the District Court would exercise jurisdiction over vendor's declaratory judgment claim.

Motion granted in part and denied in part.

Procedural Posture(s): Motion to Dismiss for Failure to State a Claim.

Attorneys and Law Firms

***1329** Kamal Ghali, Matthew Sellers, Bondurant Mixson & Elmore, LLP, Atlanta, GA, for Plaintiff.

Craig H. Kuglar, The Law Office of Craig Kuglar, LLC, Atlanta, GA, for Defendants.

ORDER

STEVE C. JONES, UNITED STATES DISTRICT JUDGE

This matter appears before the Court on Defendants' Motion to Dismiss the Complaint. Doc. No. [18]. [1] Plaintiff has responded (Doc. No. [19]), and Defendants have replied (Doc. No. [23]). This matter is now ripe for review.

I. BACKGROUND

Plaintiff filed the instant action against Defendants on June 3, 2020, seeking declaratory relief and damages arising out of a real estate transaction. See generally Doc. No. [1]. [2] In February 2020, Plaintiff, a citizen of California, listed for sale a house she owned in Clayton County, Georgia. Id. at 26, ¶ 82. Shortly thereafter, Plaintiff received from Defendant Cherwenka a proposed Purchase and Sale Agreement (the "Contract") offering to purchase the house at the list price of $125,000. Id. ¶¶ 86–87; Doc. No. [1-3]. The Contract stipulated that "30% OF PURCHASE PRICE [WAS] TO BE PAID WITH TROPTIONS.GOLD CRYPTOCURRENCY (POC)." Doc. Nos. [1], p. 27, ¶ 91; [1-3], p. 8. Attached to the Contract was a "Proof of Funds" showing the amount in Defendant Best Buy's checking account as well as an information sheet on Troptions with the heading, "Go to www.TroptionsXchange.com for more Information." Doc. Nos. [1], pp. 26–27, ¶¶ 89–90, 93; [1-3], pp. 10–11. [3] Plaintiff alleges that based on the representations in the Contract and

after speaking with her broker, she accepted Defendants' offer to purchase her home believing that she would receive the full purchase price in cash. Doc. No. [1], pp. 28–29, ¶¶ 98–105.

Plaintiff alleges that she was not told until March 6, 2020, the day of closing, ***1330** that she would need to open a "cryptocurrency wallet" to receive payment. Id. at 29–30, 33, ¶¶ 100, 106, 109, 124. She also alleges that Defendants, the closing attorney, and her own broker refused to assist Plaintiff in verifying or exchanging the funds in the cryptocurrency wallet. Id. at 30, 32–33, ¶¶ 108, 122–123, 127. Plaintiff contends that she did not finalize the closing paperwork that weekend. Id. at 33, ¶ 128. Instead, Plaintiff consulted with an attorney "who advised her that he suspected that the transaction involved securities fraud and that she should not proceed without further investigation." Id. ¶ 129. Following an email exchange between Defendant Cherwenka and Plaintiff's broker and attorney, Plaintiff refused to finalize the closing. Id. at 34, ¶¶ 130–134. In response, Defendant Best Buy filed a contract action against Plaintiff and a lis pendens with respect to her property in Georgia state court on March 11, 2020. Id. at 34–35, ¶¶ 134–135. Plaintiff ultimately removed that action to this Court; Defendant Best Buy then voluntarily dismissed the action. Id. at 35, ¶¶ 139–140.

Plaintiff asserts that she has remained liable for mortgage payments on the home and has lost the rental income she received due to the lis pendens. Id. ¶ 138. She further alleges that she has suffered economic damages and has had difficulty selling her property as a result of Defendants' actions in connection with the transaction to purchase her home. Id. at 35–36, ¶¶ 142–145. In her Complaint, she asserts claims for declaratory judgment, fraud, negligent misrepresentation, promissory estoppel, litigation expenses, and violations of the Georgia Uniform Securities Act (the "GUSA") and the Georgia RICO Act. See generally Doc. No. [1]. Defendants filed a Motion to Dismiss the Complaint for failure to state a claim pursuant to Federal Rules of Civil Procedure 12(b)(6) and 9(b). Doc. No. [18]. The court rules as follows.

II. LEGAL STANDARD

Pursuant to Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss a complaint for failure to state a claim upon which relief may be granted. Fed. R. Civ. P. 12(b)(6). A complaint has failed to state a claim if the facts as pled do not state a claim for relief that is plausible on its face. Ashcroft v. Iqbal, 556 U.S. 662, 687, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 561–62, 570, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). Labels, conclusions, and formulaic recitations of the elements of the cause of action "will not do." Twombly, 550 U.S. at 555, 127 S.Ct. 1955. To state a plausible claim, a plaintiff need only plead "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Iqbal, 556 U.S. at 678, 129 S.Ct. 1937. "Asking for plausible grounds ... does not impose a probability requirement at the pleading stage; it simply calls for enough fact to raise a reasonable expectation that discovery will reveal evidence of [the claim]." Twombly, 550 U.S. at 556, 127 S.Ct. 1955. "[W]hile notice pleading may not require that the pleader allege a specific fact to cover every element or allege with precision each element of a claim, it is still necessary that a complaint contain either direct or inferential allegations respecting all the material elements necessary to sustain a recovery under some viable legal theory." Fin. Sec. Assurance, Inc. v. Stephens, Inc., 500 F.3d 1276, 1282–83 (11th Cir. 2007) (quotations omitted).

Additionally, the Federal Rules of Civil Procedure impose a heightened pleading standard for fraud claims. Fed. R. Civ. P. 9(b). Under Rule 9(b), a party alleging fraud "must state with particularity the circumstances constituting fraud" but may allege scienter generally. Id. To plead fraud with particularity, a plaintiff must allege

> ***1331** (1) precisely what statements or omissions were made in which documents or oral representations; (2) the time and place of each such statement and the person responsible for making (or, in the case of omissions, not making) them; (3) the content of such statements and the manner in which they misled the plaintiff; and (4) what the defendant obtained as a consequence of the fraud.

FindWhat Inv. Grp. v. FindWhat.com, 658 F.3d 1282, 1296 (11th Cir. 2011). "In short, the plaintiff must plead facts that when taken as true establish the who, what, when, where, how and why of the fraud." C & C Fam. Tr. 04/04/05 ex rel. Cox-Ott v. AXA Equitable Life Ins. Co., 44 F. Supp.

3d 1247, 1254 (N.D. Ga. 2014) (citing Garfield v. NDC Health Corp., 466 F.3d 1255, 1262 (11th Cir. 2006)), aff'd, 654 F. App'x 429 (11th Cir. 2016). The heightened pleading standard of Rule 9(b) is important because it "serves the dual purpose of ensuring that a complaint 'alert[s] defendants to the precise misconduct with which they are charged and protecting defendants against spurious charges of immoral and fraudulent behavior.' " TTCP Energy Fin. Fund II, LLC v. Ralls Corp., 255 F. Supp. 3d 1285, 1289 (N.D. Ga. 2017) (quoting Ziemba v. Cascade Int'l, Inc., 256 F.3d 1194, 1202 (11th Cir. 2001) (internal punctuation omitted)).

III. DISCUSSION

In their Motion to Dismiss, Defendants argue that the Merger Clause bars Plaintiff's claims for fraud, negligent misrepresentation, promissory estoppel, and securities fraud, and prohibits reliance on predicate acts of fraud upon which to base her RICO claim. See Doc. No. [18-1], pp. 12–15. Plaintiff responds that the Merger Clause does not bar her claims because (1) the Contract itself contains the misrepresentations at issue and (2) the Merger Clause is unenforceable because the Contract, as a whole, is void. Doc. No. [19], pp. 27–30. [4]

A merger clause is a provision stating that the written agreement is the "entire agreement of the parties." First Data POS, Inc. v. Willis, 273 Ga. 792, 794–95, 546 S.E.2d 781, 784 (2001). Typically, if a contract contains a merger clause, then "prior or contemporaneous representations that contradict the written contract cannot be used to vary the [contract's] terms," and the violation of any such extraneous agreement would not "amount to actionable fraud." Id.; see also C & C Fam. Tr. 04/04/05 ex rel. Cox-Ott, 44 F. Supp. 3d at 1256 ("A merger or integration clause essentially operates as a disclaimer of all representations not made on the face of the contract."). But a merger clause has no effect when the entire contract is invalid "since, in legal contemplation, there is no contract between the parties." del Mazo v. Sanchez, 186 Ga. App. 120, 126, 366 S.E.2d 333, 337 (1988). Here, Plaintiff asserts the Contract is invalid on the grounds of fraud, illegality, and mistake. Doc. Nos. [19], p. 28; [1], pp. 36–38, ¶¶ 146–155.

A. Enforceability of the Merger Clause

"In Georgia, '[a] contract *to do* ... an illegal thing is void.' But a contract does not fall within this principle unless its ***1332** object or purpose is illegal." Smith v. Saulsbury, 286 Ga. App. 322, 333, 649 S.E.2d 344, 347 (2007) (quoting O.C.G.A. § 13-8-1). "[F]or the purpose or object of a contract to be illegal, thereby making the contract void, the contract must require a violation of law when performed." Hays v. Adam, 512 F. Supp. 2d 1330, 1342 (N.D. Ga. 2007) (citing Shannondoah, Inc. v. Smith, 140 Ga. App. 200, 202, 230 S.E.2d 351, 352 (1976)).

A contract that contemplates the sale of unregistered securities is void "[b]ecause the act of performance under the contract[ ] necessarily result[s] in violation of ... securities laws." Hays, 512 F. Supp. 2d at 1342. Plaintiff asserts that Troptions are an unregistered security and that by stipulating that a portion of the purchase price to be paid in Troptions, the Contract constitutes a sale of unregistered securities in violation of the GUSA. Doc. No. [19], pp. 12–15, 28–29.

Georgia law prohibits a person from selling or offering to sell unregistered securities in the state. [5] O.C.G.A. § 10-5-20. Both federal and Georgia law state that an investment contract is a type of security. O.C.G.A. § 10-5-2(31); cf. 15 U.S.C. §§ 77b(a)(1), 78c(a)(10). However, "investment contract" is not statutorily defined under either Georgia or federal law. Cherokee Funding LLC v. Ruth, 342 Ga. App. 404, 408, 802 S.E.2d 865, 869 (2017). The United States Supreme Court has devised a test for determining whether a particular scheme constitutes an investment contract under federal law, and the Supreme Court of Georgia has adopted that test. Id.

1. Definition of Investment Contract

Under the test, an investment contract results from (1) an investment of money (2) in a common enterprise (3) with the expectation of profits to come solely from others' efforts. SEC v. W.J. Howey Co., 328 U.S. 293, 298–99, 66 S.Ct. 1100, 90 L.Ed. 1244 (1946). The investment of money "need not be made in cash." Beranger v. Harris, No. 1:18-CV-05054-CAP, 2019 WL 5485128, at *3 (N.D. Ga. Apr. 14, 2019). Rather, the first prong is satisfied where "an investor commits assets to an enterprise or venture in such a manner as to subject himself to financial losses." Id.

The second prong is satisfied "where the 'fortunes of the investor are interwoven with and dependent upon the efforts and success of those seeking the investment or of third parties.' " Eberhardt v. Waters, 901 F.2d 1578, 1580 (11th Cir. 1990) (quoting Villeneuve v. Advanced Bus. Concepts Corp., 698 F.2d 1121, 1124 (11th Cir. 1983)). In other words, a common enterprise exists if its investors expect that a third party would be responsible for performing the chores necessary for a return. Id. at 1580–81. [6]

The third prong focuses on the investor's dependence "on the entrepreneurial ***1333** or managerial skills of a promoter or other party." SEC v. Merch. Cap., LLC, 483 F.3d 747, 755 (11th Cir. 2007) (quoting Gordon v. Terry, 684 F.2d 736, 741 (11th Cir. 1982)). In Beranger, the court found that the plaintiff-investors only had the ability to buy the security and could not manage any of the tasks required to increase its value. 2019 WL 5485128, at *3. Rather, "[t]hey could only hope that the defendants would do so effectively and that the value of the [security] would increase." Id. at *3–4.

i. Investment of money

Here, Plaintiff offered to sell her home for $125,000. Doc. No. [1], p. 26, ¶ 84. The Contract stated that Defendants would purchase Plaintiff's home for the list price, paying $87,500 in cash and the remaining 30% with "Troptions.Gold Cryptocurrency (POC)." Doc. No. [1-3], pp. 2–3, 8. For the Troptions to constitute an investment contract, Plaintiff need not have received the cryptocurrency in exchange for cash. See Beranger, 2019 WL 5485128, at *3 ("It is well-established that the 'investment of money' required for an investment contract need not be made in cash ...."). Plaintiff committed an asset—$125,000 real property interest—and was to receive in return $87,500 in cash and the equivalent of $37,500 in Troptions cryptocurrency. Doc. No. [1], p. 26, ¶¶ 84, 87. Moreover, Troptions are generally available to purchase for monetary value both online and at in-person events. See Doc. No. [1], pp. 20, 22, ¶¶ 64, 68. This proposed exchange of assets was sufficient to constitute an investment of money. Thus, the Court finds that the first prong is met.

ii. Common enterprise with the expectation of profits to come solely from the efforts of others

The Complaint further alleges that Defendant Cherwenka attached an information sheet on Troptions to his offer to purchase Plaintiff's home. Doc. No. [1], p. 27, ¶ 93; see Doc. No. [1-3], p. 11. That information sheet contains several statements including that "Troptions has purchased over 1.8 billion dollars of assets using Troptions," "people use the coins to purchase goods and services," "Troptions can be used daily for your needs," "Troptions continues to go up in value each day," and "[i]f Airbnb and Troptions.gold go on the public exchanges, you will be able to liquidate them." See Doc. Nos. [1], pp. 27–28, ¶ 95; [1-3], p. 11. It also states that "Troptions offers educational workshops" and "has a team of proven experts you can contact and get your questions answered." See Doc. Nos. [1], pp. 27–28, ¶ 95; [1-3], p. 11. The information sheet's heading refers the reader to "[g]o to www.TroptionsXchange.com for more Information." Doc. No. [1], pp. 27, ¶ 93; see Doc. No. [1-3], p. 11.

Plaintiff alleges that the Troptions website states that "Troptions are designated ... a commodity by the Commodity Futures Trading Commission," "can be ... traded in a marketplace in exchange for cash," "have a 'cash price on exchange,' " "can buy Cars, Real Estate, Business, Hotel Rooms, Gems, and many other things," and are "growing in value and liquidity each and every day." Doc. No. [1], pp. 10–11, ¶ 29. The website also allegedly states that Troptions are "serviced and managed by TROPTIONS CORPORATION," which "exists to facilitate the usefulness and utility of TROPTIONS for the holders by: 1. [p]roviding education and assistance in the best practices of TROPTIONS use[;] 2. [i]ncreasing the marketplace for TROPTIONS purchases[;] [and] 3. [p]romoting increased visibility and value of TROPTIONS in national and international trading markets." Doc. No. [1], pp. 16–17, ¶ 47.

***1334** Additionally, other websites promoting Troptions state that they are "[d]eveloping an ECO-SYSTEM of vendors accepting Troptions (car dealerships, fast food chains, legal services, ATM machines etc.)"; are "coming out with a credit card this fall so you can use your TROPTIONS to purchase merchandise"; and "will 'do the due diligence for our investors,' 'purchase large quantities of coins at a discounted rate,' and 'sell the private coins to our investors below market value.' " Doc. No. [1], p. 22, ¶¶ 67–68. And a photo posted on the "Troptions Marketplace" Facebook page shows a man standing in front of a BMW with a caption that states "Just paid all Troptions for this BMW X5 in LA!!" Doc. No. [1], p. 12, ¶ 33.

The Complaint asserts that this online information about Troptions "induces investors to rely on the managerial efforts and expertise of the promoters." Doc. No. [1], p. 16, ¶ 47. It alleges that "[a]t no point ever did anyone inform [Plaintiff] how to exchange the Troptions for U.S. dollars." Doc. No. [1], p. 33, ¶ 127. Plaintiff states that she accepted the offer on the belief that Defendants would have a third party convert the Troptions into $37,500 so she could receive the full payment in cash and that she never expected to be involved in converting the cryptocurrency into dollars. Doc. No. [1], pp. 30, 32–33, ¶¶ 107, 118, 126. She further alleges that she did not know how to "get the money out of the cryptocurrency wallet" and that Defendants "expressly refused to help her do so" when asked. Doc. No. [1], pp. 32–33, ¶¶ 117, 121–122, 127.

In Beranger, the court found that "the complaint detail[ed] several ways in which [the defendant] led the plaintiffs to believe that they could expect a profit from buying the tokens" such as advertising on social media that the "tokens will be redeemable for $3.99 in 3 months, $9.99 in 12 months and $14.99 in 15 months" as well as the fact that the "tokens were for an internet platform that had not yet been launched, and it was entirely up to the defendants to make that happen," otherwise "the tokens would be worthless." 2019 WL 5485128, at *3. Here, the Complaint alleges statements that characterize Troptions as an appreciating asset and convey that Troptions holders can rely on the promoters to see an increase in value and use. Thus, the Court finds that the there is a common enterprise with the expectation of profits to come solely from others' efforts.

2. Unlawful Sale of Unregistered Securities

Accordingly, under the facts alleged in the Complaint, the Court finds that Troptions meet the definition of an "investment contract" and thus are a security under Georgia and federal law. Taking the allegations of the Complaint as true, the Court further finds that Troptions are neither a registered nor exempted security. Doc. No. [1], p. 18, ¶ 52. However, for the Contract to constitute a violation of Georgia securities law—and thus be void for illegality—it must constitute a sale of, or offer to sell, securities. See O.C.G.A. § 10-5-20.

Under Georgia law, a sale of securities includes "every ... disposition of a security ... for value." O.C.G.A. § 10-5-2(29). An offer to sell securities includes "every attempt or offer to dispose of or solicitation of ... a security ... for value." Id. Because the Contract contemplated the exchange of real property interest for Troptions, the Contract meets the definition of a sale or offer to sell securities. Thus, the Court finds that the Contract is void for illegality because performance would have required the unlawful sale of unregistered securities. See Hays, 512 F. Supp. 2d at 1342. For that reason, the Court finds that the Merger Clause is unenforceable and ***1335** thus does not preclude Plaintiff's fraud-based claims.

B. Georgia Uniform Securities Act Claim

Count V of the Complaint asserts a claim for unlawful sale of unregistered securities. Doc. No. [1], p. 44. The GUSA makes it unlawful to offer or sell unregistered securities in Georgia, O.C.G.A. § 10-5-20, and it provides a private cause of action to the purchaser of an unregistered security, id. § 10-5-58(b). [7] As discussed, the Court finds that Troptions cryptocurrency is an unregistered security and that Defendants' offer to purchase Plaintiff's home with Troptions cryptocurrency constitutes an offer to sell an unregistered security. Thus, the Court finds that the Complaint has stated a violation of O.C.G.A. § 10-5-20 and a plausible claim under the GUSA. For that reason, Defendants' Motion to Dismiss (Doc. No. [18]) is due to be **DENIED** as to Count V.

C. Georgia RICO Claim

Under Georgia law, it is "unlawful for any person, through a pattern of racketeering activity or proceeds derived therefrom, to acquire or maintain, directly or indirectly, any interest in or control of any enterprise, real property, or personal property of any nature, including money." O.C.G.A. § 16-14-4(a). A "pattern of racketeering activity" requires at least two interrelated predicate acts. O.C.G.A. § 16-14-3(4). To state a Georgia RICO claim, a plaintiff must allege facts "show[ing] that the defendant committed predicate offenses (set forth in O.C.G.A. § 16-14-3(9)) at least twice." Cobb Cnty. v. Jones Grp., P.L.C., 218 Ga. App. 149, 154, 460 S.E.2d 516, 521 (1995) (quotations omitted). [8] "[S]uch acts must be linked, but distinguishable enough to not be merely 'two sides of the same coin.' " McGinnis v. Am. Home Mortg. Servicing, Inc., 817 F.3d 1241, 1252 (11th Cir. 2016) (quoting S. Intermodal Logistics, Inc. v. D.J. Powers Co., 10 F.

Supp. 2d 1337, 1359 (S.D. Ga. 1998)). In other words, a single extended transaction cannot provide the basis for a Georgia RICO claim. See Sec. Life Ins. Co. of Am. v. Clark, 273 Ga. 44, 48, 535 S.E.2d 234, 238 (2000).

However, "there is no requirement that plaintiff suffer direct harm from each and every alleged predicate act introduced to show a pattern of racketeering activity." ***1336** InterAgency, Inc. v. Danco Fin. Corp., 203 Ga. App. 418, 424, 417 S.E.2d 46, 53 (1992). "The direct involvement with plaintiff is not the interrelatedness or 'interconnectedness' required by the Georgia statute. It is the 'pattern' which must be shown, not that plaintiff was injured by each incident of which the pattern was comprised." Id. (internal citations omitted).

Here, the Complaint alleges the following predicate acts: wire fraud, in violation of 18 U.S.C. § 1343; a sale of unregistered securities, in violation of O.C.G.A. § 10-5-20; an unregistered broker-dealer transaction, in violation of O.C.G.A. § 10-5-30; securities fraud, in violation of O.C.G.A. § 10-5-50; and residential mortgage fraud, in violation of O.C.G.A. § 16-8-102. See Doc. No. [1], pp. 39–40, ¶ 161.

As discussed above, the Complaint has sufficiently stated a claim under the GUSA for the sale of unregistered securities in violation of O.C.G.A. § 10-5-20. Additionally, under the GUSA "[i]t is unlawful for a person to transact business in this state as a broker-dealer unless the person is registered." O.C.G.A. § 10-5-30(a). Georgia law defines a "broker-dealer" as "a person engaged in the business of effecting transactions in securities for the account of others or for the person's own account." O.C.G.A. § 10-5-2(2). Taking the Complaint's allegations as true, the Court finds that Defendants were engaged in the business of effecting securities transactions without being registered as a broker-dealer. See Doc. No. [1], p. 18, ¶¶ 51, 53–54. Thus, the Court finds that the Complaint has also alleged facts showing that Defendants violated O.C.G.A. § 10-5-30 under the GUSA.

Although the basis for Plaintiff's individual GUSA claims arise from a single transaction—the sale of Plaintiff's home—the GUSA violations that serve as predicate acts for her RICO claim arise from more than one transaction. For example, the Complaint alleges that Defendants sold or offered to sell Troptions through various online platforms and in-person events as well as in connection with the sale of Plaintiff's home. See Doc. Nos. [1], pp. 4, 20, 22, ¶¶ 7, 64, 68; [19], pp. 10–11, 14. Because Plaintiff need only allege that Defendants committed at least two predicate acts that are not part of a single, extended transaction in order to state a Georgia RICO claim, the Court need not determine whether the Complaint has alleged plausible facts to support *every* alleged act of each alleged offense. Accordingly, with respect to Count II, Defendant's Motion to Dismiss (Doc. No. [18]) is **DENIED**.

D. Fraud, Negligent Misrepresentation, and Promissory Estoppel Claims

Counts III, IV, and VI of the Complaint assert causes of action for fraud, negligent misrepresentation, and promissory estoppel. See Doc. No. [1], pp. 41–46. In their Motion to Dismiss, Defendants argue that, in addition to being barred by the Merger Clause, the Complaint has failed to state claims based on fraud or misrepresentation because the alleged misrepresentations made in connection with the transaction are not actionable statements and because the Complaint fails to show justifiable reliance. Doc. No. [18-1], pp. 15–24.

1. Fraud Claim

To state a claim for fraud under Georgia law, a plaintiff must allege facts showing: "(1) the defendant knowingly made a false statement; (2) the defendant intended for the plaintiff to act or refrain from acting in reliance on that statement; (3) the plaintiff justifiably relied on the defendant's false statement; and (4) the plaintiff's reliance resulted in damage." C & C Fam. Tr. 04/04/05 ex rel. Cox-Ott, 44 F. Supp. 3d at 1253 (citing Wylie v. Denton, 323 Ga. App. 161, 168, 746 S.E.2d 689, 695 (2013)). In addition to false statements, a fraud claim may be based on the omission of a fact "if the omitting party is ***1337** under an obligation to communicate the fact." Purchasing Power, LLC v. Bluestem Brands, Inc., No. 1:12-CV-00258-WSD, 2012 WL 3065419, at *6 (N.D. Ga. July 27, 2012) (citing O.C.G.A. § 23-2-53 (1982)). [9]

As discussed above, fraud claims are subject to a heightened pleading standard. See Fed. R. Civ. P. 9(b). The Complaint must allege with particularity "the who, what, when, where, how and why of the fraud." C & C Fam. Tr. 04/04/05 ex rel. Cox-Ott, 44 F. Supp. 3d at 1254 (citing Garfield v. NDC Health Corp., 466 F.3d 1255, 1262 (11th Cir. 2006)). Also, the alleged misrepresentations must be not only material

but also actionable; otherwise, a party is not justified in relying upon them. GCA Strategic Inv. Fund, Ltd. v. Joseph Charles & Assocs., Inc., 245 Ga. App. 460, 464, 537 S.E.2d 677, 682 (2000). Statements that are not actionable are those "constating of mere expressions of opinion, hope, expectation, puffing, and the like; rather, representations of this nature must be inquired into and examined to ascertain the truth." Id. [10] "To be actionable, [a misrepresentation] must relate to an existing fact or past event. Fraud cannot consist of mere broken promises, unfilled predictions or erroneous conjecture as to future events." Fuller v. Perry, 223 Ga. App. 129, 131, 476 S.E.2d 793, 796 (1996) (citations omitted). Additionally, a "fact is material if its existence or nonexistence is a matter to which a reasonable man would attach importance in determining his choice or action in the transaction in question." Greenwald v. Odom, 314 Ga. App. 46, 55, 723 S.E.2d 305, 315 (2012) (quoting McKesson Corp. v. Green, 299 Ga. App. 91, 94, 683 S.E.2d 336, 339–40 (2009)).

The Complaint identifies several statements and omissions Defendants allegedly made in connection with the sale of Plaintiff's home. It alleges that Defendants "made these false representations or omissions [with scienter and] with the intent to induce [Plaintiff] to sell her home." Doc. No. [1], p. 42, ¶¶ 169–172. It asserts that Plaintiff

> justifiably relied on Best Buy's and Cherwenka's false representations, in that, among other things, she believed a closing attorney would provide her with the full purchase price in U.S. dollars irrespective of how Best Buy and Cherwenka paid, and she further believed she would have a way of exchanging Troptions for U.S. dollars if she provided Best Buy and Cherwenka a "crypto wallet."

***1338** Doc. No. [1], p. 42, ¶ 173. The Complaint further alleges that Plaintiff also relied on conversations with her real estate broker, the presence of a closing attorney, and her understanding of California real estate transactions. Doc. No. [1], pp. 28–29, ¶¶ 98, 101–102. The Complaint also alleges that Plaintiff suffered damages because of Defendants' fraud. Doc. No. [1], pp. 35–36, 42, ¶¶ 142–145, 174.

The Court notes that Plaintiff's acceptance of Defendants' offer was the act that the allegedly fraudulent misrepresentations induced. However, some of the allegedly false statements that the Complaint identifies were made after Plaintiff had accepted the offer and signed the Contract. For example, Defendant Cherwenka's alleged misrepresentation that "Troptions are not security" and omission regarding the dismissal of the Missouri Secretary of State's enforcement action were made on March 10, 2020, four days after closing was to occur. Doc. No. [1], p. 34, ¶¶ 131–133. Even assuming these representations were false or materially misleading, the Complaint makes clear that Plaintiff did not take any action in reliance on them as she refused to finalize the closing. Doc. No. [1], p. 34, ¶ 134. Nor did Plaintiff rely on the closing paperwork's allegedly false representation that the Troptions were valued at $37,500 as that, too, was made after Plaintiff signed the Contract. Doc. No. [1], pp. 31–32, ¶¶ 113–114, 119. Thus, these representations do not provide a basis for Plaintiff's fraud claim.

The Complaint also alleges that Defendants' offer incorporated not only all representations contained in the Troptions information sheet attached to their offer but also all representations made on the Troptions website because the information sheet's heading says to "[g]o to www.TroptionsXchange.com for more Information." Doc. No. [1], p. 27, ¶ 93; see Doc. No. [1-3], p. 11; see also Doc. No. [1], pp. 10–11, ¶ 29 (identifying misrepresentations on the website). Even assuming that those statements can be attributed to Defendants, only some of them present an actionable basis for fraud. [11] And although the representations are included in the Complaint, the Complaint does not allege that Plaintiff had ***read and relied upon*** these representations when she accepted Defendants' offer. Moreover, Plaintiff alleges that she was concerned about the cryptocurrency and expressed those concerns to her broker. Doc. No. [1], p. 28, ¶ 97. Thus, even if the Complaint had alleged that Plaintiff read the information sheet and the website, it fails to allege how those representations misled her as required to state a fraud claim with particularity. See FindWhat Inv. Grp., 658 F.3d at 1296. Therefore, these representations also cannot provide a basis for fraud.

In admitting that she relied, at least in part, on her broker's representations, Plaintiff alleges that her broker made those representations "based on her understanding of Cherwenka's offer and her discussion with Cherwenka of the terms of the offer." Doc. No. [1], p. 29, ¶ 99. Under Georgia law,

a plaintiff may base her fraud claim on a misrepresentation to a third party if the defendant "having as his objective to defraud [the plaintiff], and knowing that [the plaintiff] will rely upon [the third party], fraudulently induces [the third party] to act in some manner on which [the plaintiff] relies." UWork.com, Inc. v. Paragon Techs., Inc., 321 Ga. App. 584, 599, 740 S.E.2d 887, 898 (2013) (quoting ***1339** Fla. Rock & Tank Lines, Inc. v. Moore, 258 Ga. 106, 107, 365 S.E.2d 836, 837 (1988)). Thus, Plaintiff could base her fraud claim on misrepresentations that Defendants made to her broker; however, she must still plead fraud with particularity. See Fed. R. Civ. P. 9(b). The Complaint does not identify any misrepresentations allegedly made by Defendants to Plaintiff's broker.

The Complaint further alleges that "Cherwenka specifically wrote in the offer that the offer included ... a business checking account statement for Best Buy Homes, LLC showing Best Buy had $285,907.12 available as of January 31, 2020," and that this account statement "was designed to give the impression that [Plaintiff] would receive $125,000 cash for the house." Doc. No. [1], pp. 26–27, ¶¶ 89–90. Plaintiff asserts that based, in part, on this statement, she "understood that she would receive $125,000 in cash if she accepted [Defendants'] offer" and she "signed the offer on [that] understanding." Doc. No. [1], p. 29, ¶¶ 104–105. However, the Complaint does not allege whether the checking account statement was false. And because the offer clearly states that part of the purchase price would be paid in cryptocurrency (Doc. No. [1-3], p. 8), this Court cannot conclude that Defendants made any material omission in connection with the checking account statement.

Plaintiff alleges that she was misled by the closing attorney's presence that there would be an independent party who would verify the funds. Doc. No. [1], p. 29, ¶ 102. She asserts that Defendants failed to disclose that Defendant Cherwenka "regularly worked with the closing attorney on real estate deals." Id. ¶ 103. But Plaintiff has not alleged that she would not have accepted the offer had she known this fact. Nor has she alleged that Defendants intentionally concealed this fact to gain a benefit. See Purchasing Power, LLC, 2012 WL 3065419, at *6. The Complaint also alleges that the offer did not define "Troptions.Gold Cryptocurrency (POC)" and that "no one provided ... a parol definition of that term." Doc. No. [1], p. 27, ¶ 92. However, the Complaint does not allege how this omission misled Plaintiff nor why Plaintiff would be justified in relying on such an omission.

For the foregoing reasons, Plaintiff has failed to state a claim for fraud because she has not plead with particularity supporting facts. Therefore, Count III of the Complaint is due to be **DISMISSED**.

2. Negligent Misrepresentation Claim

"[T]o state a claim for negligent misrepresentation, the plaintiff must allege facts showing that (1) the defendant negligently provided false information to foreseeable persons, known or unknown, including the plaintiff; (2) the plaintiff reasonably relied on this false information; and (3) the plaintiff's reliance proximately caused an economic injury." C & C Family Trust 04/04/05 ex rel. Cox-Ott, 44 F. Supp. 3d at 1253 n.4 (citing Home Depot U.S.A. v. Wabash Nat'l Corp., 314 Ga. App. 360, 367, 724 S.E.2d 53, 60 (2012)). "As the Georgia courts have recognized, the reasonable reliance that is required to state a negligent misrepresentation claim is equivalent to that needed in the fraud context." Next Century Commc'ns Corp. v. Ellis, 318 F.3d 1023, 1030 (11th Cir. 2003). "[T]he only real distinction between negligent misrepresentation and fraud is the absence of the element of knowledge of the falsity of the information disclosed." Holmes v. Grubman, 286 Ga. 636, 640–41, 691 S.E.2d 196, 200 (2010) (citations and punctuation omitted). Thus, courts generally apply the "same principles ... to both fraud and negligent misrepresentation cases" under Georgia common law. Id. "However, the heightened pleading standards of Rule 9(b) do not apply to claims of negligent misrepresentation." ***1340** In re Equifax, Inc., Customer Data Sec. Breach Litig., 371 F. Supp. 3d 1150, 1177 (N.D. Ga. 2019). [12]

Even without imposing Rule 9(b)'s heightened pleading requirements, however, the Court finds that Plaintiff has failed to state a plausible claim for negligent misrepresentation. To state a plausible claim, a complaint must allege facts showing "more than a sheer possibility that a defendant has acted unlawfully." Iqbal, 556 U.S. at 678, 129 S.Ct. 1937. Here, the Complaint refers to the statements made on the information sheet and the Troptions website but does not allege that Plaintiff read, let alone relied on, any of those representations. In fact, the Complaint states Plaintiff relied on her broker's representations after Plaintiff had concerns about the cryptocurrency. [13] Doc. No.

[1], p. 28, ¶¶ 97–98. Although the Complaint alleges that the broker's representations were based on conversations between Defendant Cherwenka and the broker, the Complaint does not allege that Defendants made any misrepresentations in their conversations with Plaintiff's broker. See Doc. No. [1], p. 29, ¶ 99. For the reasons discussed above, Count IV of the Complaint is due to be **DISMISSED**.

3. Promissory Estoppel Claim

The elements of a promissory estoppel claim are: "(1) the defendant made a promise to the plaintiff; (2) the defendant should have known that the plaintiff would rely on the promise; (3) the plaintiff did in fact rely on the promise, to [her] detriment; and (4) injustice can only be avoided by enforcement of the promise." Peery v. CSB Behav. Health Sys., No. CV106-172, 2008 WL 4425364, at *9 (S.D. Ga. Sept. 30, 2008) (citing Mitchell v. Ga. Dep't of Cmty. Health, 281 Ga. App. 174, 179, 635 S.E.2d 798, 804 (2006)). The existence of a valid contract generally bars a claim for promissory estoppel if the terms of the contract give rise to the claim. See Bank of Dade v. Reeves, 257 Ga. 51, 52, 354 S.E.2d 131, 133 (1987); see also Bouboulis v. Scottsdale Ins. Co., 860 F. Supp. 2d 1364, 1379 (N.D. Ga. 2012) ("Georgia law bars a claim for promissory estoppel in the face of an enforceable contract."). But a claim for promissory estoppel is not barred if "the promise was made in a contract that is not legally enforceable." Hendon Props., LLC v. Cinema Dev., LLC, 275 Ga. App. 434, 439, 620 S.E.2d 644, 649 (2005). Thus, the Contract does not bar Plaintiff's promissory estoppel claim because the Court determined that, under the facts as alleged in the Complaint, the Contract is void for illegality.

Here, Plaintiff asserts that Defendants "promised to purchase [Plaintiff's] home at the list price of $125,000 in cash." Doc. No. [1], p. 45, ¶ 191. The Court finds that there was a promise to purchase the home for $125,000; however, the Complaint alleges that the offer stipulated that 30% of the purchase price was to be paid with cryptocurrency. Doc. No. [1], p. 27, ¶ 91; see Doc. No. [1-3], p. 8. The offer also states that the "Purchase Price shall be paid in U.S. Dollars ... ***or such other form of payment acceptable to the closing attorney***." Doc. No. [1-3], p. 3 (emphasis added); see also Doc. No. [1], p. 28, ¶ 98 ("Shea's broker told her '[a]s long as the attorney ***1341** finds these funds acceptable, then It [*sic*] should be fine."). Accordingly, the Court finds that Defendants did not make a promise to purchase the home for $125,000 ***in cash***, and the Complaint thus fails to state a claim for promissory estoppel. Thus, Count VI of the Complaint is due to be **DISMISSED**.

E. Declaratory Judgment Claim

Count I of the Complaint asserts a claim under the Declaratory Judgment Act, 28 U.S.C. § 2201, seeking a declaration that the Contract is illegal and void and that Defendants have no interest in her property. Doc. No. [1], pp. 36–38, ¶¶ 146–155. In their Motion to Dismiss, Defendants argue that Plaintiff's declaratory judgment claim does not present a justiciable controversy as "there is no pending lawsuit against Shea," such a lawsuit is only hypothetical, and nothing currently prevents Plaintiff from selling her home. Doc. Nos. [18-1], pp. 30–32; [23], pp. 13–15. Additionally, Defendants have filed a "Suggestion of Partial Mootness" in which they allege that Plaintiff's declaratory judgment claim is moot because (1) Defendants "notified Plaintiff in writing that [they] would not be seeking specific performance 'nor will they take any other legal action to block any potential sale of the property,' " and (2) Plaintiff has since sold the property at issue. Doc. No. [23], pp. 2–3, ¶¶ 4, 8.

In response, Plaintiff argues that there is a live, justiciable controversy because Defendants still have a live breach of contract claim against her and threat of suit is not hypothetical as Defendants had previously filed a suit in state court for breach of the Contract. See Doc. Nos. [19], pp. 30–32; [28]. Plaintiff's arguments are consistent with the allegations in her Complaint. The Complaint alleges that Defendant Best Buy filed a contract action in state court in March 2020, Plaintiff removed that action to this Court on May 28, 2020, and Defendant Best Buy then voluntarily dismissed its action without prejudice on June 3, 2020. Doc. No. [1], pp. 34–35, ¶¶ 134, 139–140 (citing Best Buy Homes, LLC v. Shea, No. 1:20-cv-2276-SCJ, Doc. No. [4] (N.D. Ga. June 3, 2020)).

"Generally, the [Declaratory Judgment] Act allows prospective defendants to sue to establish non-liability, or affords a party threatened with liability an opportunity for adjudication before its adversary commences litigation." Melton v. Century Arms, Inc., 243 F. Supp. 3d 1290, 1308 (S.D. Fla. 2017). The Court agrees with Plaintiff that because Defendants may refile their breach of contract claim and seek damages, a live controversy still exists. However, "district courts possess discretion in determining whether and when to entertain an action under the Declaratory Judgment Act, even when the suit otherwise satisfies subject matter jurisdictional

prerequisites." Wilton v. Seven Falls Co., 515 U.S. 277, 282, 115 S.Ct. 2137, 132 L.Ed.2d 214 (1995).

The Eleventh Circuit has provided a non-exhaustive list of factors to consider in determining whether to proceed with a declaratory judgment action:

> (1) the strength of the state's interest in having the issues raised in the federal declaratory action decided in the state courts;
>
> (2) whether the judgment in the federal declaratory action would settle the controversy;
>
> (3) whether the federal declaratory action would serve a useful purpose in clarifying the legal relations at issue;
>
> (4) whether the declaratory remedy is being used merely for the purpose of "procedural fencing"—that is, to provide an arena for a race for *res judicata* or to achieve a federal hearing in a case otherwise not removable;
>
> ***1342** (5) whether the use of a declaratory action would increase the friction between our federal and state courts and improperly encroach on state jurisdiction;
>
> (6) whether there is an alternative remedy that is better or more effective;
>
> (7) whether the underlying factual issues are important to an informed resolution of the case;
>
> (8) whether the state trial court is in a better position to evaluate those factual issues than is the federal court; and
>
> (9) whether there is a close nexus between the underlying factual and legal issues and state law and/or public policy, or whether federal common or statutory law dictates a resolution of the declaratory judgment action.

Ameritas Variable Life Ins. v. Roach, 411 F.3d 1328, 1331 (11th Cir. 2005). [14]

Here, declaratory judgment as to the Contract's enforceability would resolve any outstanding issues between the Parties. And there is no evidence to suggest that the purpose of filing this action was an attempt at forum-shopping or "procedural fencing." Plaintiff filed this federal action after Defendant Best Buy dismissed its earlier contract action, which it had done after Plaintiff had removed the case to federal court but before Plaintiff could answer. Doc. No. [28], p. 3; see Doc. No. [1], p. 35, ¶¶ 139–140. She asserts that her declaratory judgment claim raises "all the defenses that [Plaintiff] intended to assert in [Defendants'] original breach of contract action." Doc. No. [28], p. 3. And because there is no pending litigation in state or federal court, there is no risk of increased friction between the federal and state courts nor encroachment on state jurisdiction by entertaining the declaratory judgment claim.

However, resolution of Plaintiff's declaratory claim would primarily be a question of Georgia contract law, and thus this Court's decision would most likely affect only state law. [15] Further, "courts generally decline to entertain the declaratory judgment count" where it "would serve no useful purpose because the issues will be resolved by another claim." Organo Gold Int'l, Inc. v. Aussie Rules Marine Servs., Ltd., 416 F. Supp. 3d 1369, 1376 (S.D. Fla. 2019). [16] In deciding whether the Merger Clause bars Plaintiff's fraud-based claims, this Court has determined that the Contract was unenforceable and void due to illegality. But, as discussed above, this ***1343** Court found that those claims are due to be dismissed for other reasons. Plaintiff's remaining RICO and GUSA claims would not resolve the issue at the heart of the declaratory judgment claim: whether the Contract is enforceable. For the foregoing reasons, this Court finds it appropriate to exercise jurisdiction over Plaintiff's declaratory judgment claim.

F. Bad Faith and Stubborn Litigiousness Claim

The last count of Plaintiff's Complaint, Count VII, asserts a claim for "bad faith and stubborn litigiousness" and seeks attorney's fees under O.C.G.A. § 13-6-11. Doc. No. [1], pp. 46–47, ¶¶ 197–199. The statute authorizes an award of attorney's fees "where the plaintiff has specially pleaded and has made prayer therefor and where the defendant has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense, the jury may allow them." O.C.G.A. § 13-6-11. "A request for attorney's fees under § 13-6-11 is considered specifically pled if it references the statute 'or the criteria set forth therein.' " Iroko Partners Ltd. v. Devace Integrated LLC, No. 1:12-CV-01194-SCJ, 2014 WL 11716168, at *10 (N.D. Ga. Jan. 6, 2014) (quoting Dep't of Transp. v. Ga. Television Co., 244 Ga.App. 750, 536 S.E.2d 773, 776 (2000)).

"However, simply invoking § 13-6-11 is insufficient. If unsupported by an underlying cause of action, a request for attorney's fee under § 13-6-11 is not viable." Id.; see

Gilmour v. Gates, McDonald & Co., 382 F.3d 1312, 1316 (11th Cir. 2004). "The fact that [a plaintiff] has pleaded its claim for litigation expenses in a separate count ... from its other claims for relief ... is irrelevant." Tri-State Consumer Ins. v. LexisNexis Risk Sols., Inc., 858 F. Supp. 2d 1359, 1371 (N.D. Ga. 2012). "[W]hat matters is that [the plaintiff] seeks litigation expenses related to a cause of action set forth in its other substantive counts. Thus, [the plaintiff's] ability to state a claim under O.C.G.A. § 13-6-11 depends on whether it has stated at least one viable substantive claim in its [complaint]." Id.

Defendants only address Count VII in a footnote in their brief in support of their Motion to Dismiss. Doc. No. [18-1], p. 10 n.8. Thus, their only argument with respect to Count VII is that O.C.G.A. § 13-6-11 is "not an independent cause of action and therefore does not state a claim." Id. As stated above, this Court will dismiss Plaintiff's claims for fraud, negligent misrepresentation, and promissory estoppel. However, Plaintiff's GUSA, RICO, and declaratory judgment claims remain and may provide a basis for Plaintiff's claim for litigation expenses. See Tri-State Consumer Ins., 858 F. Supp. 2d at 1371.

IV. CONCLUSION

For the reasons discussed above, Defendants' Motion to Dismiss (Doc. No. [18]) is **DENIED** as to Counts I, II, V, VII and **GRANTED** as to Counts III, IV, and VI. Counts III, IV, and VI are hereby **DISMISSED without prejudice**.

IT IS SO ORDERED this 30th day of March, 2021.

All Citations

533 F.Supp.3d 1321

Footnotes

1 All citations are to the electronic docket unless otherwise noted, and all page numbers are those imprinted by the Court's docketing software.

2 Defendant Cherwenka is the manager, a member, and the authorized agent of Defendant Best Buy Homes, LLC ("Best Buy"). Doc. No. [1], pp. 2, 8, ¶¶ 4, 22. The Complaint does not identify any other members or managers of Best Buy with whom Plaintiff had contact. For simplicity, the Court will at times refer to acts of either Cherwenka or Best Buy as acts of "Defendants."

3 The Contract also contained a provision stating that the Contract was the "sole and entire agreement between all of the parties, supersede[d] all of their prior written and verbal agreements and shall be binding upon the parties and their successors, heirs and permitted assigns. No representation, promise or inducement not included in [the Contract] shall be binding upon any party hereto." Doc. No. [1-3], p. 6. The Court refers to this provision as the "Merger Clause."

4 A motion to dismiss usually must be converted into a motion for summary judgment when a district court considers matters outside the pleadings. Fed. R. Civ. P. 12(d); Day v. Taylor, 400 F.3d 1272, 1275–76 (11th Cir. 2005). Nevertheless, a district court may consider exhibits attached to the complaint on a 12(b)(6) motion because exhibits are part of the pleadings. Fed. R. Civ. P. 10(c); Thaeter v. Palm Beach Cty. Sheriff's Office, 449 F.3d 1342, 1352 (11th Cir. 2006). Because Plaintiff attached the Contract and related documents to her Complaint as exhibits, the Court may properly consider them without converting Defendant's Motion to Dismiss into a motion for summary judgment.

5 An offer to sell is made in Georgia—regardless of whether either party is present in Georgia—if it either "(1) [o]riginates from within this state; or (2) [i]s directed by the offeror to a place in this state and received at

the place to which it is directed." O.C.G.A. § 10-5-79(c). Defendant Cherwenka's offer to purchase Plaintiff's home—and thereby his offer to sell securities—was made from Georgia. See Doc. No. [1-3], p. 9.

6 In Eberhardt, the defendant argued that the return success of investors in his cattle embryo business "was determined by how well the investor exercises the option of whether ... to utilize [the defendant's] management services." 901 F.2d at 1581. The Eleventh Circuit, however, found that it was "unlikely that an average investor would be in a position to assume or maintain any substantial degree of control over the investment" where the plaintiff "had no experience with cattle" and "significant technical expertise [would be] required if an investor intend[ed] to take possession and successfully maintain the embryos at a facility other than at [the defendant's]." Id.

7 While O.C.G.A. § 10-5-20 makes it unlawful to "offer or sell" an unregistered security, the GUSA statute creating a private cause of action provides that "[a] person is liable to the purchaser *if the person sells* a security in violation of [O.C.G.A. §] 10-5-20. O.C.G.A. § 10-5-58(b) (emphasis added). While the transaction contemplated in the Contract appears not to have occurred, Plaintiff alleges in her Complaint that Defendants "sold and offered to sell Shea Troptions." Doc. No. [1], p. 44, ¶ 184. Furthermore, Defendants have not moved to dismiss on the ground that Plaintiff has no cause of action because no unregistered security was sold. Thus, because the Court must accept Plaintiff's allegations as true at this stage, the Court finds that Plaintiff has properly pled an action pursuant to O.C.G.A. § 10-5-58(b) because Defendants "sold" Troptions to Shea.

8 "The Eleventh Circuit has advised that the particularity requirement for fraud under Rule 9(b) applies to fraud-based state RICO claims brought in a federal court." Fortson v. Best Rate Funding, Corp., No. 1:13-CV-4102-CC, 2014 WL 11456286, at *6 (N.D. Ga. Sept. 2, 2014) (citing Curtis Inv. Co. v. Bayerische Hypo-und Vereinsbank, AG, 341 F. App'x 487, 493–94 (11th Cir. 2009)); see also Peterson v. Merscorp Holdings, Inc., No. 1:12-CV-00014-JEC, 2012 WL 3961211, at *7 (N.D. Ga. Sept. 10, 2012) ("[I]f a plaintiff raises ... R.I.C.O. claims based on predicate acts of fraud, the plaintiff must comply not only with the plausibility [standard] articulated in Twombly and Iqbal, but also with Federal Rule of Civil Procedure 9(b)'s heightened pleading standard.").

9 "The obligation to communicate may arise from the confidential relations of the parties or from the particular circumstances of the case." O.C.G.A. § 23-2-53. But "[t]he mere fact that one reposes trust and confidence in another does not create a confidential relationship." Trulove v. Woodmen of the World Life Ins. Soc'y, 204 Ga. App. 362, 365, 419 S.E.2d 324, 327 (1992). "The 'particular circumstances' impose a disclosure obligation in 'any case where a person intentionally concealed a fact from a certain other person, hoping thereby to derive a benefit, and knowing that only by silence and by concealing the truth would the anticipated benefit accrue.' " Purchasing Power, LLC, 2012 WL 3065419, at *6 (quoting Reeves v. B.T. Williams & Co., 160 Ga. 15, 127 S.E. 293, 295 (1925)) (citing Miller v. Lomax, 266 Ga. App. 93, 98, 596 S.E.2d 232, 239 (2004)). "To state a prima facie case of an obligation to disclose under the 'particular circumstances,' therefore, a plaintiff must allege two factors: (1) the intentional concealment of a fact (2) for the purpose of obtaining an advantage or a benefit." Id. (citing Ga. Real Est. Comm'n v. Brown, 152 Ga. App. 323, 324, 262 S.E.2d 596, 597 (1979)).

10 For example, Georgia courts hold that "a misrepresentation as to a matter of law is a statement of opinion only ... because all persons are presumed to know the law and therefore cannot be deceived by erroneous statements of law." Lakeside Invs. Grp., Inc. v. Allen, 253 Ga. App. 448, 450, 559 S.E.2d 491, 493 (2002) (internal quotations and citations omitted).

11 See, e.g., Doc. No. [1], p. 28, ¶ 95(c) ("Troptions can show you proven secrets to make the purchase you want.").

12 Compare Wilding v. DNC Servs. Corp., 941 F.3d 1116, 1127 (11th Cir. 2019) (applying Rule 9(b) to negligent misrepresentation claims "under Florida law because such claims sound in fraud") with Baker v. GOSI Enters., Ltd., 351 Ga. App. 484, 488, 830 S.E.2d 765, 769 (2019) ("Negligent misrepresentation ... sounds in tort, and, more specifically, in the law of negligence.").

13 The Complaint does not allege whether those concerns arose from the stipulation in the offer or from the representations made on either the information sheet or online.

14 "No single factor is controlling, and the court may find other factors appropriate to consider." Atl. Specialty Ins. Co. v. City of College Park, 319 F. Supp. 3d 1287, 1292 (N.D. Ga. 2018) (citing Ameritas, 411 F.3d at 1331). Additionally, "not every factor will be relevant in every case." First Mercury Ins. v. Excellent Computing Distribs., Inc., 648 F. App'x 861, 866 (11th Cir. 2016). "Even in the absence of a parallel [state court] action, application of the Ameritas factors is appropriate." Atl. Specialty Ins., 319 F. Supp. 3d 1287, 1293–94 (N.D. Ga. 2018) (citing First Mercury Ins., 648 F. App'x at 866 ("[W]e have never held that the Ameritas factors apply only when reviewing parallel actions. Indeed, nothing in the Declaratory Judgment Act suggests that a district court's discretionary authority exists only when a pending state proceeding shares substantially the same parties and issues.")).

15 The Court recognizes that Plaintiff has asserted violation of federal securities law as a ground for unenforceability of the Contract. Doc. No. [1], p. 37, ¶ 150(b). However, Plaintiff's eight other bases all rest on state law, and the overarching question—whether the Contract is void—is a question of contract law. See id. ¶ 150.

16 But see Allstate Ins. v. Auto Glass Am., LLC, 418 F. Supp. 3d 1009, 1026 (M.D. Fla. 2019) (holding that a claim for declaratory judgment that was premised on alleged violations set forth in other claims did not have to be dismissed on the basis that it was nothing more than a "mash-up" of all prior claims).

2022 WL 888655
Only the Westlaw citation is currently available.
United States District Court, N.D. California.

UNITED STATES of America, Plaintiff,
v.
APPROXIMATELY 69,370 BITCOIN (BTC), Bitcoin Gold (BTG) Bitcoin SV (BSV) and Bitcoin Cash (BCH), et al., Defendants.

Case No. 20-cv-07811-RS
|
Signed 03/25/2022

Attorneys and Law Firms

Chris Kaltsas, Claudia A. Quiroz, David Countryman, US Attorney's Office, Criminal Division, San Francisco, CA, for Plaintiff.

Rebecca Louise Wilson, Kutak Rock LLP, Irvine, CA, for Defendant Ross William Ulbricht.

ORDER GRANTING MOTIONS TO STRIKE CLAIMS, DENYING MOTION TO INTERVENE

RICHARD SEEBORG, Chief United States District Judge

I. INTRODUCTION

***1** This is a civil forfeiture action arising from the seizure of approximately 69,370 Bitcoin, Bitcoin Gold, Bitcoin SV, and Bitcoin Cash ("Bitcoin") allegedly derived from certain unlawful activity. The Bitcoin was stolen by "Individual X" from addresses at "Silk Road," which is described by the government as having been "the most sophisticated and extensive criminal marketplace on the Internet, serving as a sprawling black market bazaar where unlawful goods and services, including illegal drugs of virtually all varieties, were bought and sold regularly by the site's users." In 2013, law enforcement seized and shut down Silk Road.

In 2020, further investigation revealed that Individual X had hacked into Silk Road and through 54 transactions sent a total of over 70,000 Bitcoin to two addresses he controlled. The bulk of that Bitcoin was later transferred to another address, from which it was ultimately seized. Individual X and the creator and owner of Silk Road have both consented to the forfeiture of the seized Bitcoin.

Several entities and individuals have now come forward asserting that the seized Bitcoin, may include Bitcoin in which they have ownership rights. The government moves to strike three such claims. A fourth potential claimant moves to intervene in this action, which the government opposes. All four motions will be decided in the government's favor as none of the claimants offer anything more than implausible speculation that any of the seized Bitcoin is their property.

II. BACKGROUND [1]

According to the government, from 2011 until October 2013, when it was seized by law enforcement, Silk Road was utilized by thousands of drug dealers and other vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers, and to launder hundreds of millions of dollars derived from these illegal transactions.

The only form of payment accepted on Silk Road was Bitcoin. During its operation, Silk Road generated sales revenue totaling over 9.5 million Bitcoin, and collected commissions from these sales totaling over 600,000 Bitcoin. Silk Road used a so-called "tumbler" to process Bitcoin transactions in a manner designed to frustrate the tracking of individual transactions through the Blockchain and thereby assist with the laundering of criminal proceeds.

The creator of Silk Road, Ross Ulbricht was arrested in San Francisco on October 1, 2013, and charged in the Southern District of New York with narcotics trafficking conspiracy, computer hacking conspiracy, and money laundering conspiracy. That same day, law enforcement took down the Silk Road website and seized its servers, including all Bitcoins contained in wallets residing within them. The following day, the government filed a civil action in the Southern District of New York seeking, among other things, forfeiture of the Silk Road hidden website, any and all Bitcoins contained in wallet files residing on Silk Road Servers, and all property traceable thereto. A judgment and order of forfeiture was entered in that action in 2014.

***2** In February of 2015, a federal jury convicted Ulbricht on seven counts including conspiracy to distribute narcotics and money laundering. He was ultimately sentenced to double

life imprisonment plus forty years, without the possibility of parole.

In 2020, law enforcement officers used a third-party bitcoin attribution company to analyze Bitcoin transactions executed by Silk Road. They saw that on May 6, 2012, 54 transfers were made from Bitcoin addresses controlled by Silk Road to two Bitcoin addresses, abbreviated as 1BAD and the 1BBq. These 54 transactions were not noted in the Silk Road database as vendor or Silk Road employee withdrawals and therefore appeared to represent Bitcoin that was stolen from Silk Road.

Nearly a year later, most of the Bitcoin at 1BAD and 1BBq was transferred to an address abbreviated as 1HQ3. Other than a relatively small transfer out in 2015, the nearly 70,000 Bitcoin remained at 1HQ3 until its seizure by the government in late 2020. During that time, its value grew from approximately $14 million to over $3.5 billion.

According to an investigation conducted by the Criminal Investigation Division of the Internal Revenue Service and the U.S. Attorney's Office for the Northern District of California, Individual X was the individual who hacked into Silk Road and moved the cryptocurrency to 1BAD and 1BBq, and subsequently to 1HQ3. The investigation further revealed that Ulbricht became aware of Individual X's online identity and threatened Individual X for return of the cryptocurrency to Ulbricht. Individual X did not return the cryptocurrency.

In November of 2020, Individual X signed a Consent and Agreement to Forfeiture with the U.S. Attorney's Office, Northern District of California in which he or she consented to the forfeiture of the subject Bitcoin. That same day, the government took custody of the Bitcoin from 1HQ3. Ulbricht has also admitted that the Bitcoin is subject to forfeiture and has consented to its forfeiture.

III. DISCUSSION

A. Roman Hossain

Roman Hossain timely filed a verified claim and statement of interest pursuant to 18 U.S.C. §§ 983(a)(4)(A) & (d), and Supplemental Rules C(6)(a) & (G)(5)(a). Hossain asserts he is "the original, rightful, and innocent owner of at least 245.922 of the 69,370 Bitcoin seized by the government from ... the 1HQ3 wallet."

According to Hossain, he opened an account on the Mt. Gox Exchange [2] on or before March 1, 2012, and deposited $2,475 to purchase Bitcoin with the hope that his investment would appreciate over time. Hossain claims he held 245.92 Bitcoin at Mt. Gox, "from where it was stolen by hackers and transferred to Silk Road." Hossain contends his Bitcoin was then stolen again from Silk Road, and ultimately transferred to the 1HQ3 wallet, from which it was seized by the government.

***3** Hossain did not identify his Mt. Gox Bitcoin wallet address or account information in his claim. The government therefore served special interrogatories in accordance with Supplemental Rule G(6)(a), seeking information to ascertain Hossain's ownership interest in the seized Bitcoin, including information relating to any account held by him at the Mt. Gox exchange. Hossain objected that the interrogatories were outside the scope of Supplemental Rule G(6), provided none of the information requested, and reiterated the statements made in his claim.

"Before a claimant can contest a forfeiture, he must demonstrate standing." *Mercado v. U.S. Customs Service*, 873 F.2d 641, 644 (2d Cir. 1989). Standing is a threshold jurisdictional issue in civil forfeiture cases, *see* *United States v. Cambio Exacto, S.A.*, 166 F.3d 522, 526-27 (2d Cir. 1999), and the government is entitled to "test" the veracity of the claimant's claim of ownership and interest any time after a claim is filed. *United States v. $133,420 in U.S. Currency*, 672 F.3d 629, 642 (9th Cir. 2012) ("The issue of standing is subject to adversarial testing under Supplemental Rule G(6)(a), which gives the government the right to question the claimant regarding the 'claimant's identity and relationship to the defendant property,' and to 'gather information that bears on the claimant's standing") (internal citations omitted).

To contest a forfeiture, a claimant must demonstrate both statutory and Article III standing. *United States v. $1,181,895.00 in U.S. Currency*, 2015 WL 631394, at *2 (C.D. Cal. Feb. 12, 2015). "A claimant bears the burden of establishing Article III standing, the threshold function of which is to ensure that the government is put to its proof only where someone acting with a legitimate interest contests the forfeiture.... A claimant must therefore demonstrate that he has a sufficient interest in the property to create a case or controversy." *United States v. $41,471.00 in U.S. Currency*, 2016 WL 337380, at *1 (C.D. Cal. Jan. 6, 2016).

In a civil forfeiture proceeding, standing is satisfied if the claimant can show "a colorable interest in the property, for example, by showing actual possession, control, title, or financial stake." *United States v. Real Prop. Located at 475 Martin Lane*, 545 F.3d 1134, 1140 (9th Cir. 2008). To collect evidence on the issue of standing, Rule G(6) "broadly allows the government to collect information regarding the claimant's 'relationship to the defendant property' " through the use of special interrogatories, and "contemplates that the government may seek information beyond the claimant's identity and type of property interest." *$133,420.00*, 672 F.3d at 642. Rule G(8)(c)(1) provides that the government may move to strike a claim for failing to comply with Rule G(5) or (6), or because the claimant lacks standing. *17 Coon Creek Rd*, 787 F.3d at 973; *see also, United States v. $333,806.93 in Proceeds*, 2010 WL 3733932, at *1 (C.D. Cal. Aug. 30, 2010) (striking claim under "strict compliance" standard for failure to respond to Special Interrogatories served pursuant to Supplemental Rule G(6)); *$133,420.00 in U.S. Currency*, 672 F.3d at 635 (emphasizing that pursuant to Rule G(8)(c), at any time before trial, the government may move to strike the claimant's claim or answer if the claimant has not responded to special interrogatories propounded pursuant to Rule G(6)(a), or if the claimant lacks standing).

Here, the government contends Hossain's claim should be stricken because he refuses to provide substantive interrogatory responses and/or because he has failed to establish standing. Hossain insists that he has adequately pleaded his interest in the property, and that striking a claim for insufficient discovery responses is not warranted unless a party has been given opportunity to cure and has violated a court order to provide further responses. Hossain also points out that the government has independently been able to identify his Mt. Gox account, rendering at least that aspect of the interrogatories moot.

***4** Hossain's conclusory allegations that his stolen Bitcoin forms a part of what was seized from the 1HQ3 wallet, however, are insufficient. Hossain has not pointed to a single fact supporting his assertions that his Bitcoin was stolen from Mt. Gox and transferred to Silk Road, and then stolen *again* and transferred ultimately into the 1HQ3 wallet. To the contrary, Mt. Gox records show that on February 8, 2013, and February 9, 2013, there was a transfer of 200 BTC and 45.92 BTC out of Hossain's Mt. Gox account for a total of 245.92 BTC. This matches exactly the amount Hossain claimed was stolen from his Mt. Gox account. These transfers took place nine months *after* the subject Bitcoin was stolen from Silk Road.

Hossain's only response is that Mt. Gox is known to have been falsifying its records to coverup the fact that losses were occurring. Whatever other irregularities there may have been, Hossein cannot escape the fact that his Bitcoin was available for him to withdraw from Mt. Gox until February of 2013, and therefore cannot be part of the Bitcoin that was stolen from Silk Road that is the subject of this case.

Even apart from the timing, Hossein would have nothing other than pure speculation to suggest that his Bitcoin was transferred to Silk Road. Again, the actual evidence is that the Bitcoin stolen from Mt. Gox accounts was transferred to various places other than Silk Road.

In essence, Hossain has done nothing more than show that he owned some Bitcoin that was stolen from him, and then baldly claimed that even though the seized Bitcoin was stolen from somewhere else, some of it must be his. The timing proves otherwise, but even in the absence of the government's showing on that point, Hussain has not met his burden to show a colorable interest in the property. The motion to strike is granted.

B. Illija Matsuko

Many months after the deadline for filing claims in this matter, Illija Matsuko, a citizen of Germany filed a verified claim alleging he held at least 48 Bitcoin[3] at Silk Road under his user name "hanson5." Matsuko asserts he had deposited the Bitcoin but had never purchased any items, legal or illegal, from the Silk Road website. The Bitcoin "remained idle" in his account.

Matsuko acknowledges he was "generally aware" of the seizure and shutdown of Silk Road in 2013, "as it made headlines worldwide" and that he "most likely lost access to the user account and that he most likely lost access to his bitcoins." Matsuko contends, however, that he was "unaware of any third-party rights under U.S. law to make a claim for his legally obtain[ed] bitcoins."

Matsuko asserts that due to the rapid increase in value of Bitcoin, in May of 2021, he sought advice from counsel in Germany about the possibility of recovering the 48 Bitcoins "from the original United States Law Enforcement take down of the Silk Road marketplace." Matsuko eventually retained

U.S. counsel and learned of this action, and filed his claim shortly thereafter.

Even assuming Matsuko should be relieved from the filing deadline in this action, he has not presented a colorable claim to any of the seized Bitcoin. Matsuko does not dispute that his Bitcoin remained in his account at Silk Road and available for his use or withdrawal at all times up until the 2013 government seizure and shut down. Accordingly, it forms no part of the Bitcoin stolen from Silk Road in 2012 that was later seized in this action.

Matsuko insists that because Bitcoin held at Silk Road was treated as fungible, he has a viable claim to the seized Bitcoin. The argument is not persuasive, however, because it would in effect mean that Matsuko's Bitcoin was simultaneously held at Silk Road *and* in the 1HQ3 wallet.

***5** Finally, Matsuko's complaint that he was not given proper direct notice of his right to assert a claim at the time of the 2013 seizure is not relevant to this proceeding. There is no basis to use this case as a collateral attack on the judgment and forfeiture order entered in New York many years ago. The motion to strike is granted.

C. Battle Born Investments Company, et al.

Approximately six weeks after the filing deadline, Battle Born Investments Company, LLC; First 100, LLC; and 1st One Hundred Holdings, LLC (collectively "Battle Born"), filed a verified claim asserting ownership of the entire 1HQ3 wallet that was seized. The claim alleges that Battle Born obtained a judgment for more than $2.2 billion against a person it believed was either Individual X or was associated with Individual X. The judgment was against Raymond Ngan, who the parties now agree is *not* Individual X.

Ngan filed a bankruptcy petition. Battle Born entered into an agreement to purchase all assets of the bankruptcy estate from the Chapter 7 bankruptcy trustee. These assets included all disclosed and undisclosed property interests of the bankruptcy debtor, "wherever located and by whomever held." The sale was approved by the bankruptcy court. The order designated Battle Born a good faith purchaser of all assets of the bankruptcy estate, whether or not disclosed in Ngan's bankruptcy schedules and statements, pursuant to 11 U.S.C. section 363(m).

In a forensic review of Ngan's laptop computer, Battle Born discovered email correspondence regarding a proposed sale of Bitcoin by Ngan. When the prospective purchaser inquired as to where the Bitcoin would come from, Ngan sent an image of the 1HQ3 page on the website, blockchain.com, which is a recognized means for Bitcoin users (and anyone else) to view the current contents and entire transactional history of a given Bitcoin wallet.

It is reasonable, of course, to take Ngan's conduct as a representation by him that he owned the 1HQ3 wallet. It is not, however, sufficient to create a colorable claim by Battle Born to the seized Bitcoin. Apart from sheer speculation that Ngan may have had some association with Individual X, Battle Born can offer nothing to suggest how Ngan would have come into ownership of the Bitcoin in 1HQ3 wallet, much less lawful ownership that would have made the Bitcoin part of the bankruptcy estate. Although Battle Born insists the question of Ngan's ownership goes to the merits and is not properly resolved by a motion to strike under either summary judgment or judgment on the pleadings standards, it is Battle Born's burden to make out a colorable claim. Because it has not pleaded facts—as opposed to conclusions—that plausibly put the 1HQ3 wallet into the bankruptcy estate it purchased, the motion to strike must be granted.

D. Kobayashi

Nobuaki Kobayashi is the appointed Foreign Representative in the case of *In re: MtGox Co., Ltd. (a/k/a MtGox KK)*, U.S. Bankruptcy Court for the Northern District of Texas, Dallas Division, Case No. 14-31229. Kobayashi moves to be permitted "direct access" pursuant to 11 U.S.C. § 1509, or to intervene under Rule 24 of the Federal Rules of Civil Procedure.

Kobayashi is tasked with overseeing the collection of any U.S.-sited assets in which Mt. Gox had or has property interests in for their transfer and distribution to Mt. Gox's creditors in the Foreign Main Proceeding in Japan. Kobayashi seeks "direct access" or intervention because he speculates some of the Bitcoin stolen from Mt. Gox could have gone to Silk Road and ultimately to the 1HQ3 wallet. Particularly in light of the government's showing that the thefts from Mt. Gox did *not* go into Silk Road, such conjecture is not sufficient to support either direct access or intervention. The motion is denied.

IV. CONCLUSION

***6** The claims of Hossain, Matsuko, and Battle Born are stricken. Kobayashi's motion for direct access or to intervene is denied. [4]

IT IS SO ORDERED.

All Citations

Not Reported in Fed. Supp., 2022 WL 888655

Footnotes

1 The general background and basic facts as alleged by the government in the forfeiture complaint and presented in its briefs and declarations are not disputed by any of the claimants except as noted in the discussion.

2 Mt. Gox was a Japan-based operation that at one time was the world's largest Bitcoin intermediary and leading Bitcoin exchange, handling 70% of all Bitcoin transactions worldwide. In February of 2014, Mt. Gox suspended trading, closed its website and exchange service, and filed for bankruptcy protection from creditors. Mt. Gox announced that approximately 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time.

3 Matsuko has since acknowledged the exact figure is 47.52.

4 The government's sealing motion (Dkt. No. 73) submitted in connection with its opposition to Kobayashi's motion is granted.

The Bits and Bytes of Cryptocurrency Litigation

Graham L. Newman
Chappell, Chappell & Newman

PRESENTATION ROADMAP

I. What is cryptocurrency?

II. How does it work?

III. Cryptocurrency and the Law

IV. Where Crypto and the Law Are Heading

The Many Faces of Crypto…

Crypto as a Computer Network

- Numerous computers operating on publicly-shared software
- Each cryptocurrency has its own network and software
- Holders vs. Miners

bitcoin

- Appx 50,000 miners
- Appx 170 million holders

Crypto as a Distributed Ledger

Txn Hash	Method	Age	From	To	Quantity
0x7dcb4a0707d5c437...	Stake End	23 secs ago	Null: 0x000...000	0x0BF3B7...3cb4F09E	20,443.63259632
0x7889e5e288a9426e...	Uniswap V3S...	1 min ago	0xcA74F4...D5a65597	Uniswap V3: HEX	661,699.76686915
0x80de48af64cff821b...	Transfer	1 min ago	0x48c04e...8f38a7fF	0xA38435...51110492	797,610.65285785
0x8e9c399505564b6fd...	Unoswap	2 mins ago	Uniswap V2: HEX	0xDe37c0...4Db86575	102,407.85388221
0x878f193ed63f41cf8...	Multicall	2 mins ago	Uniswap V3: HEX	0x48c04e...8f38a7fF	487,292.83208301
0x99381e772a0bcddc...	Multicall	2 mins ago	Uniswap V3: HEX	0x48c04e...8f38a7fF	307,459.66701473
0x63bac21c8a65772b...	Transfer	7 mins ago	0x083375...Eaad34B6	MEXC: Mexc.com	106,779.4326087
0x77daca91f8cfa09d0...	Multicall	9 mins ago	Uniswap V3: HEX-USDC	0xc8C870...5BC4DD49	41,540.3195901
0x974309e1f95c6e7b3...	Transfer	10 mins ago	0x00AF8a...4D1286b4	0x083375...Eaad34B6	53,707.52962272
0x4ca77b24460797a7f...	Relay Tokens	11 mins ago	0x9c0373...3F1B5EA6	PulseChain: Omnibridg...	278,426.66472856
0x00eaf93fc6cf8d7b4...	Unoswap	11 mins ago	0xDA5DD5...Cd565Bef	Uniswap V2: HEX	328,047.66919948
0xe76c05b6dc8116d7...	Transfer	21 mins ago	MEXC: Mexc.com	0x72Cac4...6f51EE8a	5,354.39

Crypto as Money

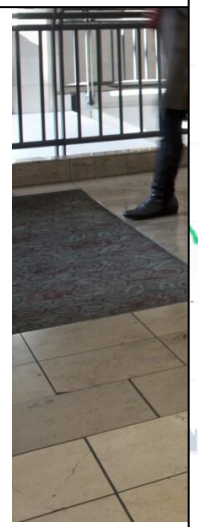
REUTERS® World Business Markets Sustainability

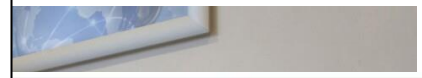
Future of Money

Amazon CEO says not ac
cryptocurrency as payme
anytime soon

Reuters

April 14, 2022 9:30 AM EDT · Updated 2 years ago





Read 327851 times)

quote #1

AM

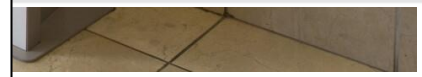
a couple of pizzas.. like maybe 2 large ones so I have some left over for
left over pizza to nibble on later. You can make the pizza yourself and
er it for me from a delivery place, but what I'm aiming for is getting food
itcoins where I don't have to order or prepare it myself, kind of like
r' at a hotel or something, they just bring you something to eat and

ppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard
or anything like that. I also like regular cheese pizzas which may be
rwise acquire.

let me know and we can work out a deal.

Report to moderator

Mv8Rh45aUet



Crypto as Investment

CRYPTOCURRENCY › INITIAL COIN OFFERINGS

The Most Successful ICO All Time

By NATHAN REIFF Updated September 23, 2021

Reviewed by ERIKA RASURE

Fact checked by KATRINA MUNICHIELLO

A company can launch an ICO to raise funds.

WSJ PRO CENTRAL BANKING

Home Analysis Interactives Regions Financial Regulation Newsletters

MARKETS

SEC Chief Fires Warning Shot Against Coin Offerings

Clayton says ICOs in many cases look like securities, suggesting companies may need to register the deals with the SEC

By Dave Michaels and Paul Vigna

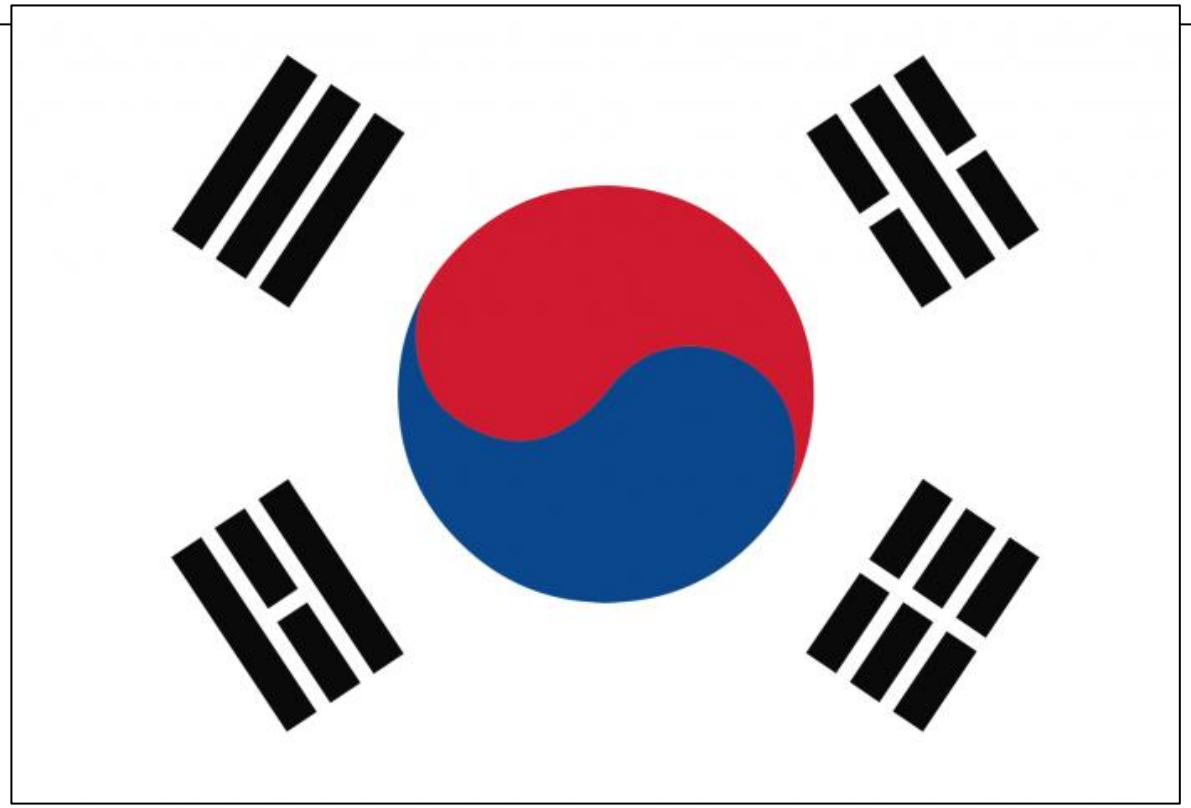
Updated Nov. 9, 2017 5:31 pm ET | WSJ PRO

Share Resize 12

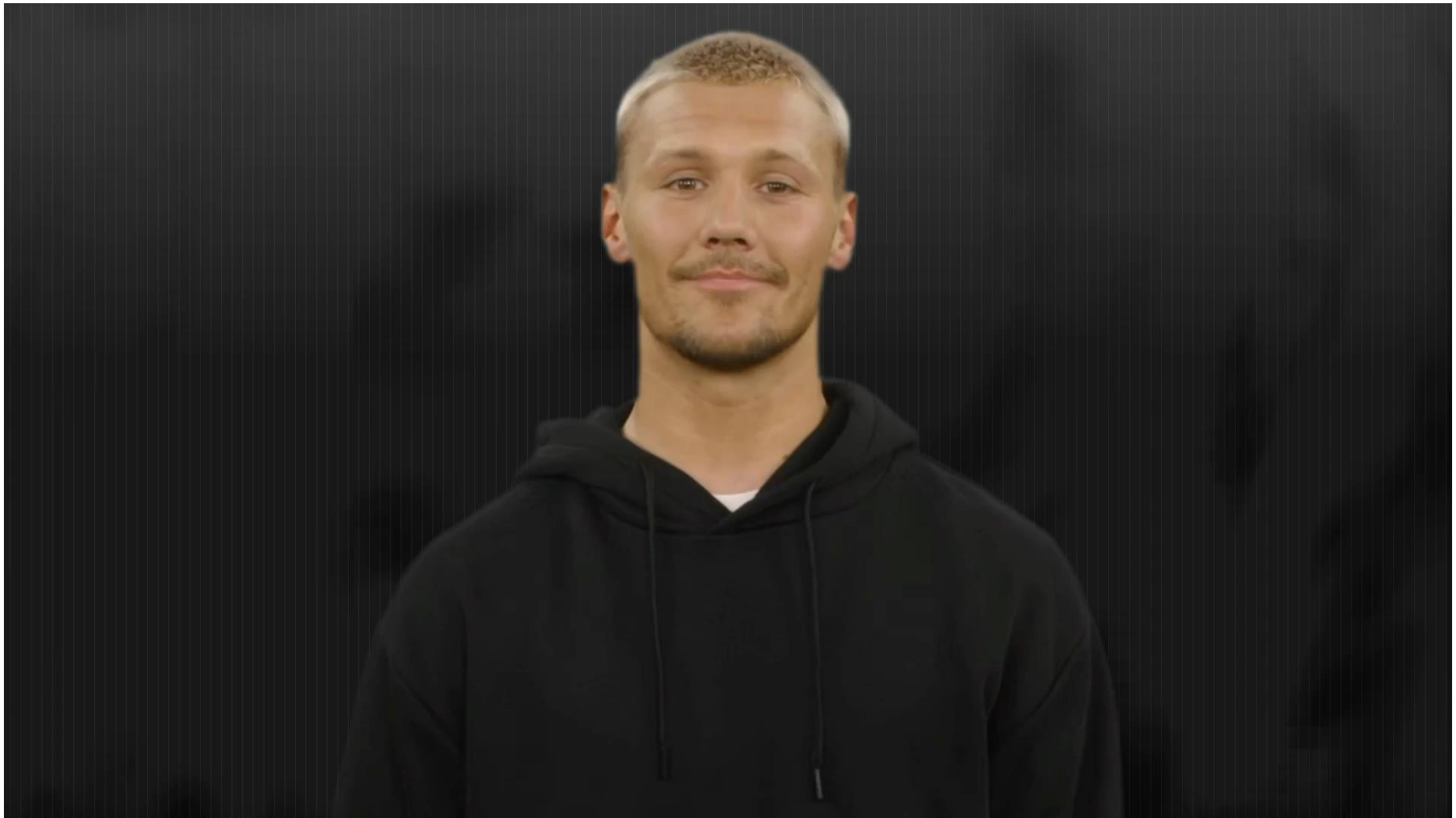
TOP NEWS & ALERTS

'It's Still Too Early' to Discuss Rate Cuts, Bank of Canada Gov. Macklem Says

#	Name	Price	1h %	24h %	7d %	Market Cap
1	Bitcoin BTC	$42,106.58	▼ 0.11%	▼ 0.58%	▼ 3.92%	$824,146,305,625
2	Ethereum ETH	$2,237.31	▲ 0.14%	▼ 0.04%	▼ 5.08%	$268,923,649,735



But how does cryptocurrency work?



Public Key Cryptography

0x0BF3B7b9267F7306fFd68cc782cd9e1f3cb4F09E

- Where “Cryptocurrency” gets its name…
- Creates a public “address” or “wallet” from which you can send or receive assets.
- All transactions from this address are visible to the public but remain pseudonymous.*
- Paired with a private key which, if kept private, ensures the validity of the transactions.

Immutable Data

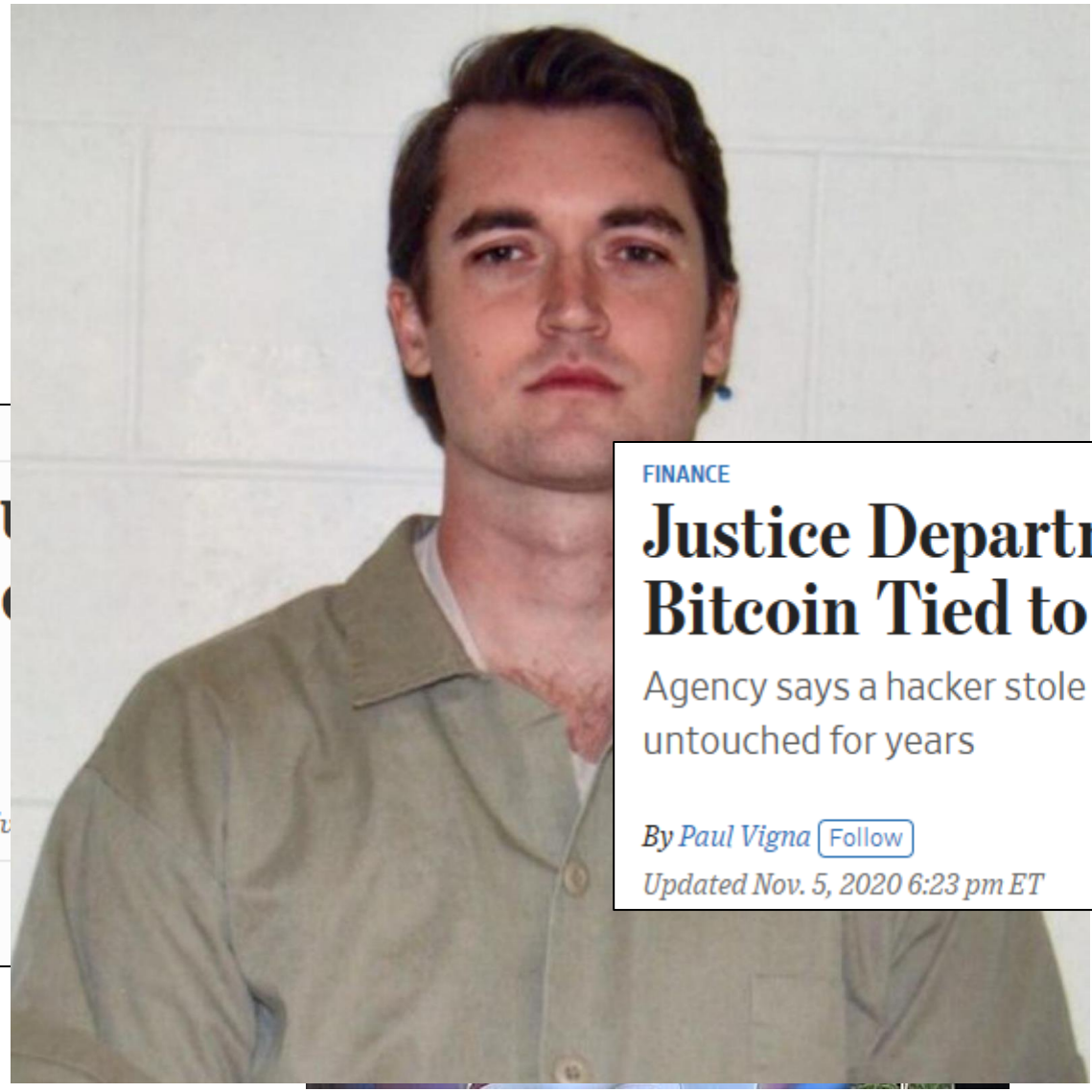
- The distributed ledger can only be added to—it cannot be changed.
- Historic record of every transaction on the network's ledger, or "blockchain."

But how do people get cryptocurrency?

Bitcoin mining

Centralized Exchanges

The Silk Road and Crypto for Criminals



FORBES > TECH > SECURITY

Founder Of Dru
Says Bitcoin B
Won't Kill His

Andy Greenberg Former Staff
Covering the worlds of data security, priv

FINANCE

Justice Department Seizes $1 Billion of Bitcoin Tied to Silk Road Website

Agency says a hacker stole funds in 2012, 2013 from drug website, left untouched for years

By Paul Vigna Follow
Updated Nov. 5, 2020 6:23 pm ET

Crypto in Family court

Coe v. Rautenberg, 358 So. 3d 24 (Fla. Dist. Ct. App. 2023)

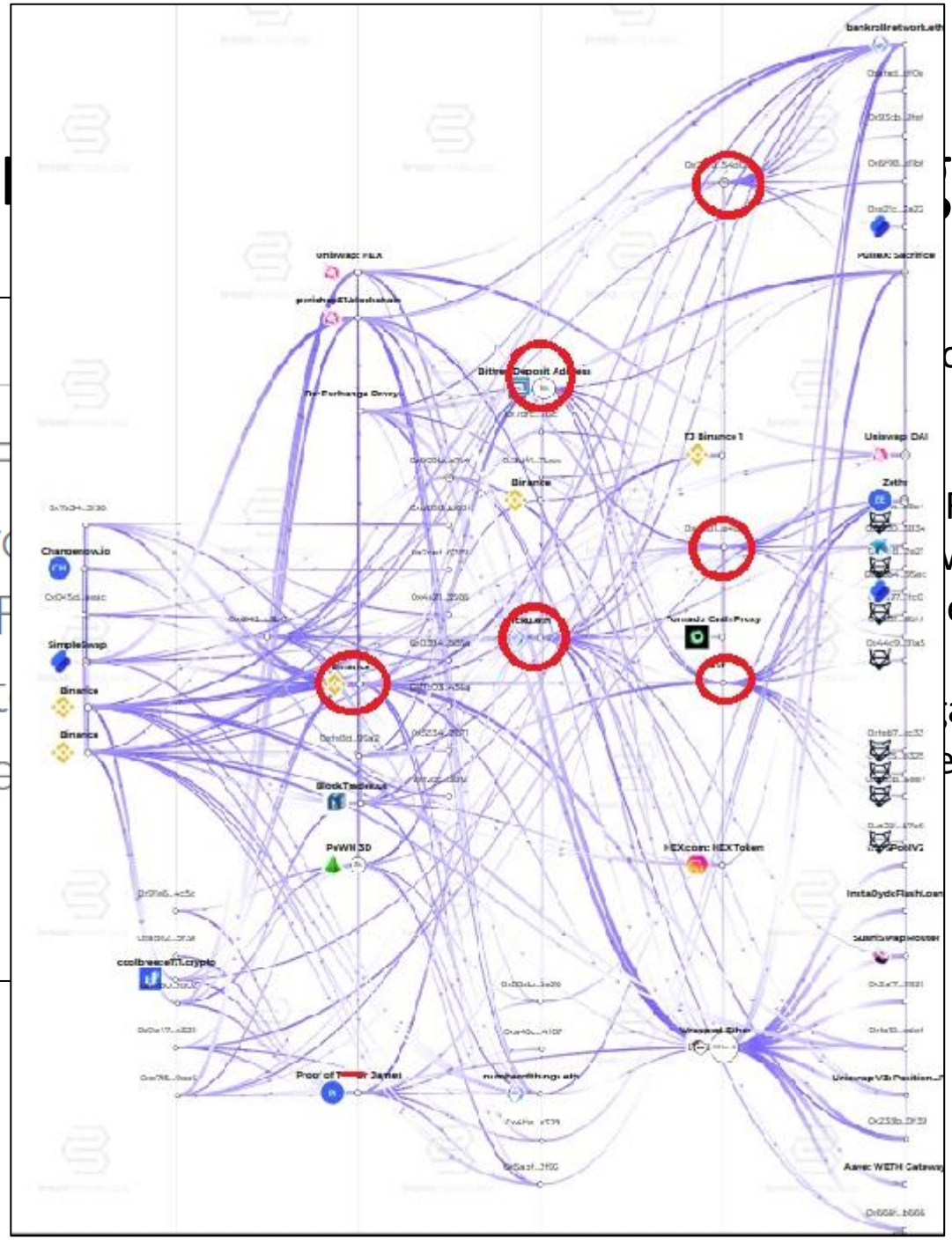
- 10 “marital Bitcoins” equitably distributed between the spouses.
- 1.2 Bitcoin ordered paid for past child support.
- Wife to be reimbursed half the cost of recovering the Bitcoin hard drive.
- Wife to receive “equivalent of $22,954.75 in Bitcoin” for additional past due child support.

Cr gation

Press Release

SEC Charges Hex F
Heart with Misappr
Dollars of Investor F
Unregistered Crypt
Offerings that Raise
Billion

FOR IMMEDIATE RELEASE
2023-143

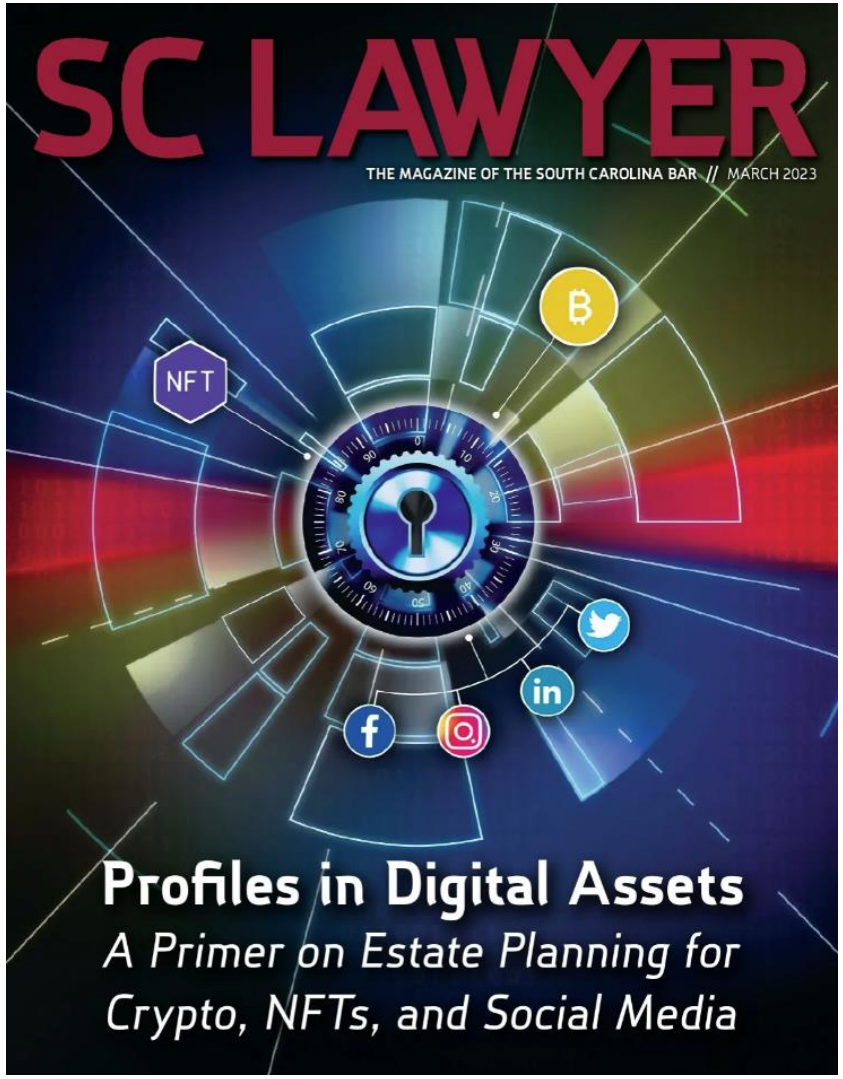


oken offering was an
security

Representations made in
with the sale of the security
ent

ations of “recycled transactions”
e impression of product demand

Crypto in Estate Planning



- Custody of Centralized Exchange accounts
- Safety of Key Pairings
- Disbursement Plans

Crypto in Real Estate

Shea v. Best Buy Homes, LLC, 533 F. Supp. 3d 1321 (N.D. Ga. 2021)

- House listed for sale for $125,000
- Buyer counters w/ 30% of purchase price to be paid in Crypto
- Seller eventually invalidates the contract as void for illegality

Crypto in Civil Litigation

HEX

“Alt-Coins”

Crypto and the Law Into the Future

- Regulation
- Web3 Economy
- Central Bank Digital Currencies

Crypto Oversight: Whose Backyard???

Blockchain

Web3 Will Run on Cryptocurrency

A Q&A with crypto expert Jeff John Roberts. by Ramsey Khabbaz

May 10, 2022, Updated May 13, 2022

Summary. What exactly is cryptocurrency — and how does it fit into the broader Web3 ecosystem? To better understand this buzzword and why it matters, HBR associate editor Ramsey Khabbaz spoke with Jeff John Roberts, a technology journalist and the author... **more**

Editor's note: We first interviewed Jeff John Roberts in April, before the May 2022 cryptocurrency crash. We spoke with him again, on May 12, to ask him about it. His comments follow the original interview.

Cryptocurrencies are having a moment, to say the least. From Elon Musk's tweets, to cryptic Super Bowl advertisements, to the freshly

Central Bank Digital Currency (CBDC)

While the Federal Reserve has made no decisions on whether to pursue or implement a central bank digital currency, or CBDC, we have been exploring the potential benefits and risks of CBDCs from a variety of angles, including through technological research and experimentation. Our key focus is on whether and how a CBDC could improve on an already safe and efficient U.S. domestic payments system.

CBDC is generally defined as a digital liability of a central bank that is widely available to the general public. Today in the United States, Federal Reserve notes (i.e., physical currency) are the only type of central bank money available to the general public. Like existing forms of money, a CBDC would enable the general public to make digital payments. As a liability of the Federal Reserve, however, a CBDC would be the safest digital asset available to the general public, with no associated credit or liquidity risk.

The Federal Reserve Board has issued a discussion paper that examines the pros and cons of a potential U.S. CBDC. As part of this process, we sought public feedback on a range of topics related to CBDC. The Federal Reserve is committed to hearing a wide range of voices on these topics.

Money and Payments: The U.S. Dollar in the Age of Digital Transformation

Summary of Public Comments on Money and Payments: The U.S. Dollar in the Age of Digital Transformation

All Public Comments on Money and Payments: The U.S. Dollar in the Age of Digital Transformation

Research and Publications

See the most recent research and publications related to central bank digital currencies.

Speeches and Testimony

See the most recent speeches related to central bank digital currencies.

FAQs

See frequently asked questions related to central bank digital currencies.

Reach Out to Me!

Graham Newman
Chappell, Chappell & Newman
graham@chappell.law