THE INTERNATIONAL ACADEMY
OF FINANCIAL CRIME LITIGATORS

SEPTEMBER 2023

Working Paper 1

Secret Notes And Anonymous Coins: Examining FinCEN's 2019 Guidance On Money Transmitters In The Context Of The Tornado Cash Indictment

Benjamin Gruenstein | Evan Norris | Daniel Barabander

Table of Contents

About the Authors

Benjamin Gruenstein

Partner
Cravath, Swaine & Moore LLP

Benjamin Gruenstein is a partner in Cravath's Litigation Department and a member of its Investigations and Regulatory Enforcement practice. He focuses on the representation of U.S. and multinational companies and their senior executives in high-stakes government and internal corporate investigations in such areas as the Foreign Corrupt Practices Act, healthcare fraud, trade sanctions, insider trading, securities and accounting fraud, and accompanying civil litigation. Mr. Gruenstein has handled both domestic and cross-border investigations, including in Latin America, Asia and Europe.

Mr. Gruenstein regularly advises clients in connection with criminal and regulatory investigations, including those conducted by the Department of Justice, the Securities and Exchange Commission and other federal and state regulatory agencies. He represents boards of directors and their committees on issues related to corporate governance and regulatory compliance and conducting independent investigations on behalf of boards and board committees. Mr. Gruenstein also routinely represents corporate clients in a broad range of civil litigation matters.

Mr. Gruenstein is a member of the American Law Institute, the Supreme Court Historical Society Board of Trustees and the International Bar Association, and a fellow of the American Bar Foundation and the International Academy of Financial Crime Litigators.

Prior to joining Cravath, Mr. Gruenstein served as an Assistant U.S. Attorney in the Criminal Division of the U.S. Attorney's Office for the Southern District of New York from 2002 to 2008.

Email: bgruenstein@cravath.com

Evan Norris

Partner
Cravath Swaine & Moore, LLP

Evan Norris is a partner in Cravath's Litigation Department and a member of its Investigations and Regulatory Enforcement practice and Data Security and Privacy practice. He focuses on advising U.S. and multinational companies and their boards and senior executives with respect to government and internal investigations, criminal

defense, regulatory compliance and related civil litigation. Mr. Norris routinely handles matters ranging from cross-border investigations and cryptoasset-related compliance reviews to cyber incident response.

An experienced trial and appellate lawyer, Mr. Norris has represented clients in a variety of sensitive matters concerning the Foreign Corrupt Practices Act, trade sanctions, cybersecurity, anti-money laundering controls, the False Claims Act and securities fraud. He is also a frequent speaker on topics ranging from cryptoasset and ESG enforcement trends to governance standards for international sports organizations. Mr. Norris also regularly publishes articles and resources, among these, "Regulatory Compliance in the Context of a Cross-Border Data Breach," which he co-authored for Global Investigation Review's "Guide to Cyber Investigations" (Second Edition) and "More than Just the Ooki DAO: Lessons for Web3 Companies About Control After bZx," which he co-authored for Coindesk (October 2022).

Prior to joining Cravath, Mr. Norris served for 10 years as an Assistant U.S. Attorney in the U.S. Attorney's Office in 2017 for the Eastern District of New York. He held a number of leadership positions during his tenure, including Chief of the National Security and Cybercrime Section, and was the lead prosecutor of the groundbreaking FIFA case, spearheading a global investigation of corruption in international soccer in one of the most far-reaching cross-border corruption cases ever brought by the Department of Justice.

Email: enorris@cravath.com

Daniel M. Barabander

Associate
Cravath Swaine & Moore, LLP

Daniel M. Barabander is an associate in Cravath's Corporate Department. His practice focuses on crypto and fintech matters, with particular attention to the intersection between detailed, often code-level, technical analysis and regulation. Before entering the legal profession, Daniel was a founder at a startup and worked at the New York Stock Exchange as an analyst.

Email: dbarabander@cravath.com

1 Introduction

On August 23, 2023, the U.S. Attorney's Office for the Southern District of New York announced the unsealing of an indictment against Roman Storm and Roman Semenov charging, among other things, conspiracy to operate an unlicensed money transmitting business in connection with their role as founders of Tornado Cash, from at least March 2022 until August 8, 2022. The criminal statute that is the object of the charged conspiracy, 18 U.S.C. § 1960(b)(l), provides that a party operates an unlicensed money transmitting business if, among other things, it fails to register with the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") when required to do so under the Bank Secrecy Act and FinCEN regulations.

In the days that have followed, commentators have been revisiting FinCEN's 2019 guidance on crypto assets, or what the agency calls "convertible virtual currencies" ("CVCs"), in an effort to better understand the indictment and, more broadly, what it means to be a money transmitter in the Web 3 context. While FinCEN makes clear up front that the guidance is not meant to "establish any new regulatory expectations or requirements," it is nonetheless arguably the best source to consult to understand FinCEN's interpretation of money transmission as applied to CVCs, as it is the most recent in-depth formal guidance FinCEN has published on the topic.[1]

Given that Tornado Cash operates as a "mixer" for crypto assets to anonymize ownership, the discourse to this point has largely focused around one particular sub-section of FinCEN's 2019 guidance that discusses the difference between providers of (1) anonymizing "services," defined as "persons that accept CVCs and retransmit them in a manner designed to prevent others from tracing the transmission back to its source," and (2) anonymizing "software," defined as "suppliers of software a transmittor would use for the same purpose."[2] This distinction is critical to whether a provider is a money transmitter: under FinCEN's guidance, the former is a money transmitter and the latter is not.

While commentators' focus on the "service" versus "software" distinction is sensible, any test based on the distinction is inherently difficult to apply because it is rooted in categorizations based on fuzzy facts and circumstances inherent to Web 3 systems like Tornado Cash, which do not abide by traditional notions of what it means to provide a ***service*** that utilizes ***software***. However, there is another section of the 2019 guidance that, while not focused on anonymizers as such, sheds light on what it means for a CVC

---

1 FinCEN, FIN-2019-G001 Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019) 1–3, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf [hereinafter FinCEN 2019 Guidance].

2 *Id.* at 19 (emphasis removed).

platform to be a money transmitter. In fact, this section—on CVC wallets—is the ***only*** section of the 2019 guidance that provides a principle-based rubric for defining money transmission: a money transmitter must exercise "total independent control" over the value being transmitted, which based on our review of the guidance and as discussed below, means that it has both necessary ***and*** sufficient control to transmit funds.

While the Tornado Cash indictment alleges how the founders controlled components of Tornado Cash, it does not allege how those components controlled the funds being transmitted. The indictment focuses on the "secret note" that customers use when depositing to and withdrawing from Tornado Cash. However, despite allegations that the secret note was transmitted through various components of Tornado Cash that the founders controlled when a customer withdrew, in reality, the customer never relinquished control over the secret note. Rather, she sent only a "proof" that revealed nothing about the secret note and could only be validated by the smart contract to send funds directly from the smart contract to the customer. As such, during the time period that the founders are alleged to have operated a money transmission business, they had at most the control necessary to transmit funds, but not sufficient control. Such limited control would appear to be insufficient for the government to establish that Tornado Cash was a money transmitter under FinCEN's 2019 guidance.

2 Legal background

The Bank Secrecy Act ("BSA") requires "financial institutions" to assist U.S. government agencies in preventing money laundering. When the law was first passed in 1970, covered financial institutions consisted solely of traditional financial actors, such as banks, brokers and dealers in securities, futures commission merchants, and mutual funds. In 1999, FinCEN instituted a final rule that defined a new type of financial institution—a "money services business"—that was meant to capture "certain non-bank financial institutions."[3] One such institution was a "money transmitter." Under a 2011 amendment to the rule, a "money transmitter" is defined as: (a) a "person that provides money transmission services" or (b) any "other person engaged in the transfer of funds."[4] While the term "engaged in the transfer of funds" is not defined, the term "money transmission services" is defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[5] If a party is a money transmitter, it must register with FinCEN and comply with a series of anti-money laundering obligations under the BSA, many of which require knowledge of the identity of customers, users and others.

---

3 *Am I an MSB?*, FinCEN, https://www.fincen.gov/am-i-msb.

4 31 C.F.R. § 1010.100(ff)(5)(i)

5 *Id.*

In 2019, FinCEN published a detailed, 30-page guidance, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," the most substantive analysis the agency has provided to date regarding Web 3 systems.[6] FinCEN's stated objective was "to remind persons . . . how FinCEN regulations . . . apply to certain business models involving . . . CVCs."[7] The guidance describes various CVC business models and sets forth the agency's view as to whether they involve money transmission services. In particular, section 4, "Guidance on Application of BSA Regulations to Common Business Models Involving the Transmission of CVC," includes sub-sections examining business models involving anonymity-enhanced CVC transactions (§ 4.5) and CVC wallets (§ 4.2) at length.

But while the discussion of anonymity-enhanced CVC transactions provides a helpful starting point, including by explaining that an anonymizing service provider is a money transmitter but an anonymizing software provider is not, this part of the guidance does not define the underpinning legal principles for this distinction. For example, it states that an anonymizing software provider is not a money transmitter because it is merely providing "the delivery, communication, or network access services used by a money transmitter to support money transmission services," an exemption cited elsewhere in the guidance.[8] But it does not discuss the underlying principles for why this exemption exists in the first place. That discussion is found in the CVC wallets section.

3 The CVC wallets section of the 2019 FinCEN guidance

The CVC wallets section of the 2019 guidance defines a rubric for determining "[t]he regulatory interpretation of the BSA obligations of persons that act as intermediaries between the owner of the value and the value itself,"[9] which is what makes a party a money transmitter. The rubric consists of four factors: "(a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the CVC runs; and, (d) whether the person acting as intermediary has total independent control over the value."[10] FinCEN then applies this rubric to CVC wallet providers, which it breaks down along two matrices: providers of unhosted versus hosted and multi-signature (multi-sig) versus single-signature (single-sig) wallets. Hosted wallet

6 FinCEN also provided formal guidance in a 2013 document titled "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." While FinCEN has commented on money services businesses more recently in other publications, it has not published new formal guidance on CVCs since 2019.

7 FinCEN 2019 Guidance 1.

8 *Id.* at 20.

9 *Id.* at 15.

10 *Id.*

providers "transmit CVCs on behalf of their accountholders," possessing a user's private key, which is in contrast to unhosted wallets where the user possesses her private key. [11] Multi-sig wallet providers "are entities that . . . for enhanced security, require more than one private key for the wallet owner(s) to effect transactions" and single-sig wallets are not multi-sig wallets.[12] The guidance concludes that multi-sig and single-sig hosted wallet providers are money transmitters because they have "total independent control" over the value, whereas unhosted multi-sig and single-sig wallet providers are not money transmitters because the provider does not have such control.[13]

Through FinCEN's assessment of these different types of wallet providers, we see the crucial point: the level of control a party has over the value being transmitted is what is determinative of whether that party is a money transmitter. FinCEN's discussion of unhosted multi-sig providers is particularly illuminating. The agency states that even if such a "provider validates and executes the transaction using the second key it houses," it still considers this to constitute the owner interacting with the payment system directly instead of through an intermediary, and therefore, the provider is ***not*** a money transmitter.[14] Put another way, even though the provider is ***necessary*** for the transfer of value to occur (by housing one of the keys required to sign the transaction), its control is not ***sufficient*** because it cannot independently transfer assets on behalf of the user (because the user houses the other key). This brings to the forefront a crucial distinction: to act as a money transmitter, a party must have necessary ***and*** sufficient control over the value being transmitted.

In fact, looking at the four factors, we can see they all collapse into the final factor (d): whether the intermediary has "total independent control" over the value. Factor (a), who owns the value, is always the owner of the wallet, so it does not impact the analysis. Factor (b), where the value is stored, draws a distinction between the owner's wallet versus the provider's wallet or private database. Whether the value is stored on the provider's wallet or in a private database is another way of asking whether the provider can unilaterally control the value with its own private keys—whether it has necessary and sufficient control. Factor (c), whether the owner interacts directly with the payment system, makes clear that a "person participating in the transaction to provide additional validation at the request of the owner does not have total independent control over the value," and thus what it means to interact directly with the payment system depends on whether the party has necessary and sufficient control over the value.[15]

---

11 *Id.*

12 *Id.* at 17. FinCEN does not technically define the term "single-signature" wallet, but wallets are either single-signature or multi-signature.

13 *Id.* at 16–17.

14 *Id.* at 17.

15 *Id.*

This focus on control makes complete sense in the context of defining a money transmitter. If the party has both necessary and sufficient control, it has truly accepted the value with the purpose of transmitting it on behalf of another, rather than simply acting as the "delivery, communication, or network access services" for a user to do so without an intermediary.[16] This conception is rooted in principle: as FinCEN states, its "guidance applies to any business model that fits the same key facts and circumstances described in the guidance, regardless of its label" because "[t]he regulatory interpretation of the BSA obligations of persons that act as intermediaries between the owner of the value and the value itself is not technology-dependent."[18] Thus, this necessary and sufficient control framework applies to any business model to determine whether it involves money transmission services. For example, in another section of the guidance discussing the decentralized exchange business model, FinCEN states that "a CVC trading platform [that] only provides a forum where buyers and sellers of CVC post their bids and offers . . . does not qualify as a money transmitter."[19] Under a control framework, it is apparent why: the forum may be necessary for the particular transfer of value to occur, but without control over the value itself, it is not sufficient.

4 Assessing the indictment against the founders of Tornado Cash

The money transmitter conspiracy count in the indictment focuses on the time period from at least March to August 2022 (¶ 80) and alleges, in sum, that the defendants, "together with others involved in the Tornado Cash service, including the relayers, engaged in the business of transferring funds on behalf of the public" as an unlicensed money transmitting business (¶ 33). However, as we discuss next, while the indictment contains detailed allegations with regard to the ways the founders exerted control over the Tornado Cash service generally, it is silent as to how the founders or their alleged co-conspirators controlled the value itself—the critical question from the perspective of FinCEN's 2019 guidance.

4.1 The allegations that the founders conspired to operate an unlicensed money transmission business

The allegations in the indictment focus on three main components that make up the Tornado Cash service. (¶ 10.)

16 *Id.* at 9.

17 *Id.* at 2.

18 *Id.* at 15.

19 *Id.* at 24.

First, there are the smart contracts that underpin the service. These smart contracts run autonomously on the blockchain. To deposit crypto assets, a customer sends her crypto assets to the smart contract through a "deposit" function, which locks them in the smart contract. To withdraw crypto assets, a customer calls a "withdraw" function on the smart contract, which unlocks her crypto assets and returns them to her. Between the deposit and the withdrawal, the customer's assets are "commingled with other customer deposits" in the smart contract, which makes drawing the connection between a specific depositor and specific withdrawer so difficult that it effectively anonymizes where the assets came from, and therefore, who owns them after they are withdrawn. (¶ 50.) While the indictment alleges that from the launch of the service in August 2019 until May 2020, the founders "exercised complete control over the Tornado Cash service" because they held "private keys" that "could further modify" the smart contracts, it goes on to allege that they relinquished their control over the smart contracts in May 2020. (¶ 26.) Therefore, the founders are not alleged to have controlled the smart contracts during the relevant period charged in the indictment for when they allegedly operated an unlicensed money transmitting business, from March 2022 to August 8, 2022.

Second, the service has a user interface ("UI"), which is the front-end website typical customers of the service use to interact with the smart contracts because it did not require "technical sophistication" to use. (¶ 13.) The indictment describes the UI as "a key component of the Tornado Cash service" because it provides helpful information to increase anonymity and makes the smart contracts and relayers accessible to the lay customer, which enhances the privacy of all customers by increasing the set of possible customers any particular crypto assets could belong to. (¶ 21.) The indictment alleges that the "founders had the ability to make changes to the UI at their own discretion" and had "control over . . . operation and design of the UI." (¶¶ 14, 26.)

Third, instead of interacting with the smart contract independently (whether through the UI or directly), customers have the option of using "relayers." A relayer is a third party who "relays" the customer's call to the withdraw function on the smart contract. The relayer's function is to front the "gas" cost required to pay for interacting with the smart contract. By fronting the gas cost, the relayer allows a customer to obtain the crypto assets she deposited into the smart contract without the need to first purchase crypto assets to cover the gas cost, which generally requires interacting with a fiat on-ramp such as a centralized exchange. Centralized exchanges require personal information to use, meaning they create a link between a wallet and a person. Relayers allow customers to avoid this interaction, which provides for more anonymity. The indictment alleges that the founders controlled the relayers by (1) launching the Tornado Cash decentralized autonomous organization ("DAO") and the associated governance token, TORN, which relayers could acquire and stake to increase their likelihood of being selected by a customer who chose to use relayers (¶ 30); and (2) "incorporat[ing] an algorithm into the

Tornado Cash UI" that managed logic for selecting relayers (¶ 29). The Tornado Cash DAO voted in favor of the plan to incorporate the algorithm in the UI in March 2022, suggesting that the relayers may be central to the government's charging theory regarding money transmittance, given that the relevant period for the charge begins in March 2022.

The allegations make clear that the founders ***controlled the UI and the relayers*** at various times, but not how they, or Tornado Cash, ***controlled the value itself***. In sum, the indictment does not allege how these components that the founders controlled equated to control over the value being transmitted, which is what is determinative of whether a party is a money transmitter under FinCEN's 2019 guidance, as we read it. This is not to say that the government cannot make such a showing, but rather that it has not done so in this indictment.

4.2 Analyzing control over the value

The indictment does not allege facts that allow a conclusion to be drawn that Tornado Cash was a money transmitter under FinCEN's 2019 guidance. Its allegations revolve around how the UI and relayers transmitted the secret note to the smart contract upon a customer's withdrawal. But there are no allegations the UI controlled the secret note, and our review of the public smart contract code demonstrates that both the UI and relayers sent a proof that revealed nothing about the secret note.

4.2.1 The allegations regarding the secret note

When a customer deposits to Tornado Cash, she must have some information that is secret to her to prove she is the one who deposited. The indictment alleges that "[t]he UI . . . would provide a unique 'secret note' to the Tornado Cash customer for each deposit, and the customer would be the only person with access to the secret note."[20] (¶ 15.) In other words, according to the indictment, (1) the customer is "the only person with access to the secret note," (¶ 15) meaning the customer never shares it with any third party; and (2) the act of using the UI to generate the secret note does not share it with any third party.

Logically, the customer must use this secret note in some way when withdrawing to prove she is the person who deposited into the smart contract. The indictment alleges that the customer "would go to . . . the UI and enter the secret note" (¶ 16) and the "UI [would] sen[d] the secret note to a smart contract" (¶ 18). Alternatively, the customer could "choose to have a Tornado Cash relayer transmit the secret note to the Tornado Cash smart contract." (¶ 24.) The indictment alleges that upon receiving the secret note, the

20 The indictment does not discuss the process of how a customer would obtain a secret note when not interacting with the UI, or use the secret note when not interacting with the UI or a relayer, but these actions would be possible to do.

"smart contract validated the secret note, and then the corresponding amount of [the applicable crypto asset] was transferred from the Tornado Cash pool to the customer-designated address." (¶ 18.)

Reviewing these allegations, we encounter a contradiction, because the "secret note" is defined as something that is kept secret by the customer, yet the indictment describes it as being shared with a public smart contract, either through the relayer or the customer herself. The secret note appears to be central to understanding control, because, according to the indictment, it is validated by the smart contract and is what permits the transfer of funds, analogous to a private key held by a hosted wallet provider on behalf of a customer. In other words, possessing the secret note on behalf of another appears to be determinative of whether a party has the requisite control over the value to be a money transmitter.

4.2.2 A technical review of how deposits and withdrawals using the secret note work

Untangling this contradiction as to the secret note requires a more technical understanding of Tornado Cash than the indictment provides. When a customer uses Tornado Cash, the customer picks a random number[21] that she does not share with any other person, including any person associated with Tornado Cash. This secret number is the "secret note." This number can be picked by the customer independently or through the UI, as the indictment alleges. However, as the indictment also alleges, picking it through the UI does not share the secret note with another party, because the customer remains "the only person with access to the secret note." (¶ 16.) This is because even when the UI is utilized, the secret note is picked "locally," meaning on the customer's own device and is not shared with any third party, including the founders.

When the customer deposits her crypto assets to the smart contract, she locally runs a one-way cryptographic hashing algorithm, passing in this secret note. This hashed value, ***which cannot be used to determine the secret note*** (why the hashing algorithm is "one-way"), is shared with the smart contract. Crucially, however, the customer does not share the secret note itself with the smart contract.

To withdraw at a later time, the customer utilizes a "zero knowledge proof." A zero knowledge proof is a cryptographic protocol used to prove something is true without revealing any information as to why it is true. Zero knowledge proofs have a "prover," who is trying to prove something is true, and a "verifier," who is verifying that the thing is true. During the withdrawal process, the customer acts as the prover and the smart contract

21 Technically, the customer picks two random numbers, which is necessary to ensure customers do not withdraw from the smart contract multiple times. For simplicity, we refer to the secret note as one number.

acts as the verifier. The customer runs a "proving algorithm" which uses cryptography to generate a "proof," a value that reveals nothing about the secret note. The customer runs this proving algorithm on her local device, passing in the secret note and other "public" inputs, such as her destination address (the address to withdraw to). Again, because this is done on the customer's device, the secret note is never shared with another party in generating the proof.

So, it is not the case, as the indictment alleges, that the "UI sen[ds] the secret note to a smart contract" (¶ 18) or the "relayer transmit[s] the secret note to the Tornado Cash smart contract" (¶ 24), nor is it the case that the smart contract "validate[s] the secret note" (¶ 18); it is the ***proof*** that the customer shares with the smart contract and it is the ***proof*** that the smart contract validates when the customer wants to withdraw her assets. In fact, the customer can send the proof to the smart contract directly or to a relayer to send to the smart contract. Along with the proof, the customer will send values that are inextricably intertwined with the proof, including the customer's destination address. Below is the `withdraw()` function on Tornado Cash's 10 ETH pool smart contract:

Figure 1: The `withdraw()` function on the 10 ETH pool smart contract.[22]

```
function withdraw(
    bytes calldata _proof,
    bytes32 _root,
    bytes32 _nullifierHash,
    address payable _recipient,
    address payable _relayer,
    uint256 _fee,
    uint256 _refund
) external payable nonReentrant {
    require(_fee <= denomination, "Fee exceeds transfer value");
    require(
        !nullifierHashes[_nullifierHash],
        "The note has been already spent"
    );
    require(isKnownRoot(_root), "Cannot find your merkle root"); // Make sure to use a recent one
    require(
        verifier.verifyProof(
            _proof,
            [
                uint256(_root),
                uint256(_nullifierHash),
                uint256(_recipient),
                uint256(_relayer),
                _fee,
                _refund
            ]
        ),
        "Invalid withdraw proof"
    );

    nullifierHashes[_nullifierHash] = true;
    _processWithdraw(_recipient, _relayer, _fee, _refund);
    emit Withdrawal(_recipient, _nullifierHash, _relayer, _fee);
}
```

22 Tornado Cash 10 ETH Pool (Code), Etherscan, https://etherscan.io/address/0x910cbd523d972eb0a6f4cae4618ad62622b39dbf#code.

This `withdraw()` function, running autonomously on the smart contract, receives in, among other values, the proof (`_proof`), the customer's destination address (`_recipient`), the relayer's address (`_relayer`) (if a relayer is used), and the fee to the relayer (`_fee`) (if a relayer is used). These values accompanying the proof were among the same "public" inputs the customer passed to the proving algorithm when generating her proof. These values are then passed to a verification function `verifier.verifyProof()`(line 17). The verification function then plays the role of the verifier in the zero knowledge proof protocol, by running the "verifying algorithm." The verifying algorithm uses cryptography to determine whether the proof is valid for the other "public" inputs (such as the customer's destination address) and whether it was generated by someone who could provide the secret note to the proving algorithm. Again, the information about the secret note is not revealed in the proof, but the proof still cryptographically guarantees that the customer knows a secret note that was used when depositing (without revealing anything about which deposit was the customer's). If this proof is valid, the `_processWithdraw()` function is called (line 32); if it is not, the program will stop running and the `_processWithdraw()` function will not be called. The `_processWithdraw()` function is the code necessary to run to transfer the customer's locked crypto assets from the smart contract to the customer and relayer. The `_processWithdraw()` function looks as follows:

Figure 2: The `_processWithdraw()` function on the 10 ETH pool smart contract.[23]

```
1  function _processWithdraw(
2      address payable _recipient,
3      address payable _relayer,
4      uint256 _fee,
5      uint256 _refund
6  ) internal {
7      // sanity checks
8      require(
9          msg.value == 0,
10         "Message value is supposed to be zero for ETH instance"
11     );
12     require(
13         _refund == 0,
14         "Refund value is supposed to be zero for ETH instance"
15     );
16
17     (bool success, ) = _recipient.call.value(denomination - _fee)("");
18     require(success, "payment to _recipient did not go thru");
19     if (_fee > 0) {
20         (success, ) = _relayer.call.value(_fee)("");
21         require(success, "payment to _relayer did not go thru");
22     }
23 }
```

23 *Id.*

Examining this code, line 17 demonstrates that the ether is sent directly from the smart contract to the customer (`_recipient`), minus a fee if a relayer was used. Line 20 demonstrates that, if there was a relayer used, the fee (in ether) is sent directly to the relayer (`_relayer`).

Accordingly, when a customer uses a relayer, she sends the proof to the relayer with specific values, including her desired destination address. The relayer then calls the `withdraw()` function, passing in these values, which validates whether the proof is valid and was generated by someone who knows the secret note (without actually receiving the secret note), which is the customer. Because the values are bound to the proof, if the relayer were to change any of these values the proof will fail verification and the `_processWithdraw()` function will never be called. If the proof is valid, the smart contract will call the `_processWithdraw()` function. This function will independently and separately send the locked up ether to the customer and to the relayer.

4.2.3 Applying the technical understanding of the secret note to control over the value

Understanding the technical underpinnings of how Tornado Cash works, and in particular how the secret note is used, is necessary to assess whether the founders actually possessed control over the value being transmitted during the period charged in the indictment.

Assuming "the customer would be the only person with access to the secret note" (¶ 16) as the indictment alleges, no party but the customer would have had necessary and sufficient control over the value. The founders had at most necessary control over the value being transferred—meaning that when the customer used Tornado Cash, the UI or the relayers that the founders allegedly controlled may have been necessary to send the message to transfer the value in that particular transaction—but not sufficient control—meaning the founders could not have transferred value independently from the customer. This is because (1) the valid proof required to unlock and transfer the funds could only be generated by the customer with the secret note, which the founders did not have access to; (2) the proof revealed nothing about the secret note; and (3) the proof was only valid for the values specified by the customer, including the destination address the customer sets. In other words, simply by sharing the proof, the customer did not provide another party "total independent control" over the value. The founders did not control the smart contract during this period, and in any event, the smart contract did not receive the secret note. Furthermore, as the indictment alleges, the founders' control over the UI did not provide them with the secret note, because this value was picked

locally on the customer's device and not shared with the founders. Finally, to the extent the founders controlled the relayers, this would not have provided them control over the secret note because the relayers never received the secret note.[24] The founders' role is roughly analogous to the unhosted multi-sig provider, which is not a money transmitter under FinCEN's 2019 guidance.

5 Conclusion

FinCEN's 2019 guidance is just that—guidance. It is not binding on FinCEN or the Department of Justice, and it does not have the force of law. Yet it remains the best resource to consult from the agency that promulgated the rules defining a money transmitter to understand, from the agency's perspective, what those rules mean in the context of crypto assets. And the guidance in particular as to CVC wallets establishes "total independent control"—which we understand to require necessary and sufficient control over value— as the defining feature underpinning money transmission analysis in decentralized systems.

While the money transmission conspiracy charge in the Tornado Cash indictment clearly alleges how the founders controlled various components of the Tornado Cash service, it does not allege that those components exercised control over the value being transmitted. Nor can it, based on our review of how the secret note actually worked during the relevant time period. While the defendants and other conspirators may have exercised necessary control over funds through the components they then controlled, they could not have exercised sufficient control to transfer funds because they did not possess the secret note. If the government is going to be bound by FinCEN guidance, it remains to be seen whether and how it will be able to establish that Tornado Cash exercised both necessary and sufficient control over funds, and thus that the founders conspired to operate it as an unlicensed money transmitting business.

---

24 The indictment alleges that the relayer "deduct[s] a fee" (¶ 24), but it is the customer—not the relayer—who sets the fee when she generates the proof, and the smart contract separately sends the customer and the relayer the funds.