Exhibit ‘A’

BITCOIN & CRYPTO FINANCIAL FORENSICS

PROFESSOR J.W. VERRET, JD, CPA/CFF, CFE, CVA

ASSOCIATE PROFESSOR, GEORGE MASON UNIVERSITY SCHOOL OF LAW

SAME FORENSIC PRINCIPLES APPLIED TO NEW ASSETS

- Standards of Forensic Accounting (for holders of the CPA/CFF certification)

  Statement on Standards for Forensic Services No. 1 (including due professional care, sufficient relevant data, integrity and objectivity)

- Standards of Fraud Examination (for holders of the CFE certification)

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- Financial Forensic standard tools available include:
  - Net Worth/Income Indirect Analysis
  - Presence of Unexplained Assets
  - Correlation/Pattern Analysis
  - Money Laundering Habits/Typology
  - Crypto Privacy Behavior Patterns

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- Note on Blockchain Tracing for purposes of this question:

Mr. Sterlingov has been open about the fact that, like many users, he used Bitcoin Fog for personal privacy. To the extent the government presents evidence using tracing, skepticism about those tools presented in evaluating Claim II below applies here in Claim I regarding issues with their reliability and error rate.

The government has not shown exactly how many bitcoin they believe were the total Mr. Sterlingov mixed through Bitcoin Fog, but 1600 BTC is roughly the estimate implied by the Scholl Report.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

Note on Blockchain Tracing for purposes of this question (continued)

High Risk of DOUBLE COUNTING of total Bitcoin owned by Sterlingov in the Scholl Report.

Using the 1600 BTC estimate of total mixed funds for the sake of discussion does not grant legitimacy to the use of the government's Chainalysis tracing tools in this respect or to the government's totals. I only give weight to admissions by Mr. Sterlingov that, like other Bitcoiners, he used Bitcoin Fog for privacy.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- Early Bitcoin buyers and adopters experienced incredible returns and obtained Bitcoin partly outside the documented financial system in peer-to-peer exchanges or personal Bitcoin mining (it was certainly easier for individuals to successfully mine in 2010 and 2011).
- Mr. Sterlingov's Bitcoin activity began 12-13 years ago, when extraordinary returns make subsequent forensic tracing difficult, particularly for bitcoiners with off-exchange activity.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

Bitcoin & Traditional Assets ROI (vs USD)

	Bitcoin	Gold	S&P 500
1 year:	+35%	+14%	+14%
2 year:	-22%	+9%	+4%
3 year:	+185%	+3%	+41%
4 year:	+215%	+39%	+51%
5 year:	+271%	+61%	+62%
6 year:	+997%	+56%	+84%
7 year:	+4,480%	+47%	+110%
8 year:	+10,128%	+80%	+117%
9 year:	+4,963%	+51%	+130%
10 year:	+32,008%	+49%	+169%
11 year:	+341,646%	+22%	+228%
12 year:	+221,320%	+21%	+253%
13 year:	+47 million%	+67%	+314%
14 year:	+3.9 billion%	+111%	+366%

https://casebitcoin.com

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- As a Certified Public Accountant also Certified in Financial Forensics and as a Certified Fraud Examiner, I am required to consider alternative explanations by CFF and CFE standards.
- A sense of the state of Bitcoin and the Bitcoin community in 2010, when Mr. Sterlingov first started buying and receiving Bitcoin, is demonstrated by Bitcoin Pizza Day.
- On May 22, 2010, an individual paid 10,000 Bitcoin in exchange for 2 pizzas. Those 10,000 Bitcoin would be worth roughly $300,000,000 ($300 million) today. That was the first time Bitcoin was used in a commercial transaction and is remembered by Bitcoiners as Bitcoin Pizza Day.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- An individual with Mr. Sterlingov's assets and salary would be able to easily afford 1,600 Bitcoin in 2010 (assuming govt's implied assertion that roughly 1600 BTC is the correct total for Bitcoin belonging to Mr. Sterlingov that utilized the Bitcoin Fog privacy tool) and early 2011 when the price was as low as $.40 cents for an extended period, much lower at times, and otherwise under a dollar for the first quarter of 2011. (https://www.forbes.com/advisor/investing/cryptocurrency/bitcoin-price-history/)

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- He could have reasonably received 1600 bitcoin as hobbyist transfers at early meetups in 2010 and 2011 for free.

- High Risk of DOUBLE COUNTING of total Bitcoin owned by Sterlingov in the Scholl Report.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- Sterlingov's trading patterns (buying historic lows, selling historic highs) could have magnified his early Bitcoin appreciation for any pattern inference, particularly since it appears to have been mostly off-exchange.
- High Risk of DOUBLE COUNTING of total Bitcoin owned by Sterlingov in the Scholl Report.
- All information in the government's evidence is consistent with Sterlingov purchasing all the Bitcoin he owns with his salary and/or his Bitcoin and later crypto trading profits. It is also consistent with his Bitcoin holdings resulting in large part from the receipt of hobbyist transfers early in Bitcoin's history.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- Sterlingov's financial records do not fit the patterns of money laundering for three reasons….

- **Reason 1**
  - sending post-mix tokens from a privacy tool like Bitcoin Fog back to a KYC-complaint venue like Kraken would put the real operator of Bitcoin Fog at risk of prosecution, yet the author of bitcoinfog.com is clearly expert in privacy tools and tactics

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- Sterlingov's financial records do not fit the patterns of money laundering for three reasons….
- **Reason 2**
- The true operator of Bitcoin Fog would have earned $600,000,000 ($600 Million) worth of Bitcoin in today's value, or an amount of fees valued at $1,400,000,000 ($1.4 Billion) at Bitcoin's highest historical price. There is no sign of wealth of that scale in Mr. Sterlingov's financial history. Where did it go?

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- Sterlingov's financial records do not fit the patterns of money laundering for three reasons….
- **Reason 3**
- No evidence that Sterlingov's Malta "To The Moon VPN" company, that accepted bitcoin from a prospective user base of private VPN customers, was used for the integration stage of classic money laundering. Nothing found on the company's servers or in its financial records indicates it was used for that purpose.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- **THE MISSING BITCOIN**
- It seems from the Scholl Report that the subtotal of funds the government alleges was the total amount of Bitcoin that Mr. Sterlingov used the Bitcoin Fog privacy tool for appears to be approximately 1600 BTC. (this total wasn't given to us by the government, I had to guess at what they would allege)
- High Risk of DOUBLE COUNTING of total Bitcoin owned by Sterlingov in the Scholl Report.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- The prosecution alleges that funds received to Mr. Sterlingov's cryptocurrency exchange accounts are "proceeds" from Bitcoin Fog, implying that these deposits are from the operation of the service.
- The government's evidence provides no evidence linking those funds to the operation of Bitcoin Fog, all the evidence I have reviewed indicated that accusation by the government is nothing but speculation.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- The government appears to presume that merely using Bitcoin Fog to protect personal privacy is illicit. This is not so, as a pretrial ruling by the Court in this action has previously described.
- It would not be clear to an everyday user of Bitcoin Fog that simply using the Bitcoin Fog tool is somehow illicit.
- Reports by Chainalysis and by international government banking and economic regulators and by the United Nations indicate that the rate of illicit funds sent through bitcoin mixers is similar to the rate of illicit money laundering that regularly takes place in traditional banks.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- An evaluation of the total "proceeds" that could have been expected to accrue to the administrator of Bitcoin Fog over the lifetime of operating the service is summarized below. On page 2 of the Statement of Facts, the prosecution states that Bitcoin Fog processed "over 1.2 million BTC."
- Applying a 2% service fee, as discussed by the prosecution on page 11 of the Statement of Facts, the expected proceeds are as followed on the next slides. (Real world proceeds of Bitcoin Fog to its operator may be higher, toward a 3% fee, which would magnify the mystery of the missing bitcoin)

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- When including the total BTC directly or indirectly received by Sterlingov from Bitcoin Fog and the remaining BTC in the broader Bitcoin Fog cluster, the prosecution has failed to account for over **$600,000,000 ($600 Million) in current value of Bitcoin that the administrator of Bitcoin Fog should have received.**

- **This valuation stretches to $1,400,000,000 ($1.4 Billion) at the height of Bitcoin's market value.**

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- The **MISSING BITCOIN** in this case amounts to over **21,000 BTC, which is 13X** more than the amount that has been alleged by the government to have been received by Sterlingov from addresses linked to Bitcoin Fog.
- That is $600,000,000 ($600 Million) to $1,400,000,000 ($1.4 billion) US dollars that is MISSING from the government's case in value depending on when you historically apply a value to the **MISSING BITCOIN**.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- Bitcoin Fog Operations Proceeds Accounting
- BTC Processed by Fog alleged by Government 1,200,000 BTC
- Fee Rate Estimate 2.0% (conservative, could stretch to 3%)
- Total Fees Received By Operator 24,000 BTC (conservative, may stretch toward 36,000 BTC)
- Govt Est. of Sterlingov Bitcoin Sourced From Bitcoin Fog 1600.36 BTC
- Approximate BTC Remaining in the Bitcoin Fog Cluster 1305.47 BTC
- **"Proceeds" Unaccounted For 21,094.17 BTC (worth $632 million in todays dollars, worth $1.4 Billion at Bitcoin's price peak in 2021)**

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES?

- **Conclusions From Bitcoin Fog Transaction Fee Accounting**
- Despite claims that they completed a thorough accounting of the activity of Bitcoin Fog and the activity of Sterlingov's deposits to his cryptocurrency exchange accounts, ***the prosecution falls short of the expected proceeds of the operator of Bitcoin Fog by an order of magnitude of conservatively 13 times*** the amount of Bitcoin that the prosecution can show Mr. Sterlingov ever possessed, and perhaps the prosecution misses on a much higher magnitude.
- **In my opinion, the deposit profile and activity of Sterlingov's cryptocurrency exchange accounts are not indicative of having been anything more than an early adopter of cryptocurrency and user of the Bitcoin Fog service in an effort to maintain his privacy.**

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- Usage of Bitcoin Fog to mix Bitcoin does not necessarily indicate illicit activity, large Bitcoin holders are at increased risk of kidnapping, surveillance, privacy violations, as DOJ prosecutions demonstrate
- Privacy is important in the Bitcoin community
- Bitcoin Privacy Tools are used by citizens in oppressive regimes around the world to avoid government surveillance and human rights abuses

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- Pattern/Correlation Analysis
  - Insufficient evidence to establish a pattern or correlation between Bitcoin Fog operator's transaction fees and Mr. Sterlingov's Bitcoin activity, due to the size difference between them.
  - Bitcoin Fog's fees are 13 TIMES larger than Sterlingov's cumulative Bitcoin holdings that have gone through Bitcoin Fog as alleged by the government.

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- Pattern/Correlation Analysis Continued…
  - Indications of off exchange Bitcoin activity by Sterlingov not in government's evidence suggest early Bitcoin purchases simply moved through Bitcoin Fog
  - High Risk of DOUBLE COUNTING of total Bitcoin owned by Sterlingov in the Scholl Report.
  - To the extent a pattern is discernible, Mr. Sterlingov's Bitcoin activity began in the early 2010-2011 period where magnitude price appreciation is extraordinary (exponential), while Bitcoin Fog transaction activity didn't peak until 2012-2013 and later gain momentum

EVALUATING CLAIM 1: DID STERLINGOV RECEIVE BITCOIN FOG FEES

- Net worth/Net Income Analysis
  - Useful to find hidden assets or sources of income (though does not indicate whether illicit)
  - Insufficient evidence for government net worth/net income analysis typical in money laundering forensics
  - High Risk of DOUBLE COUNTING of total Bitcoin owned by Sterlingov in the Scholl Report.
  - No credible indication of unexplained real-world wealth, **particularly on the necessary scale of $600 Million to $1.4 Billion**

RESULTS FOR CLAIM I: DID STERLINGOV RECEIVE BITCOIN FOG FEES? NO INDICATION HE DID

- **No indication Sterlingov received Bitcoin Fog Fees for 7 reasons**
  - Insufficient evidence for Net Worth/Net Income Indirect Analysis
  - Lack of Substantial Unexplained Assets (Relative to Bitcoin Fog total fees at one point valued at over $1.4 BILLION, presently valued at $600 MILLION)
  - Lack of Pattern Correlation Between BTC Fog fees and Sterlingov Bitcoin activity
  - Sterlingov's early bitcoin wealth explainable
  - Use of privacy tool explainable
  - Doesn't fit money laundering pattern, To The Moon LLC wasn't used for integration of laundered funds, why not? To the Moon LLC appears to instead simply be a failed business venture
  - Sending post-mix tokens to Kraken account out of character for level of privacy skill of BitcoinFog.com operator

CRYPTO FINANCIAL FORENSIC INQUIRY FOCUS MOVES TO THE SECOND CLAIM

After analyzing whether Mr. Sterlingov received fees from Bitcoin Fog, the second part of my inquiry moves to whether Chainalysis' tracing can be relied upon to attribute ownership of Bitcoin at an address, including at an address in a chain of transactions alleged to be self-transfers, to Mr. Sterlingov.

My perspective before joining this case was that blockchain tracing of the type used by Chainalysis was useful for the initial stages of financial forensic investigations to generate leads. I understood however that it was alone insufficient to attribute ownership of crypto like Bitcoin to an individual. My perspective is supported in the prior literature.

EVALUATING CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS

- High error rate in blockchain tracing tools suggested in literature, the error rate is itself highly variable owing to fact that the literature is very new
- "Two heuristics, multi-input and one-time change, are applied. The multi-input and one-time change heuristics yield average error rates of 63.46% and 92.66%, respectively. The application of both heuristics yields the lowest average error rate of 57.47%." *Gong et al*

EVALUATING CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS

- ”Tracers in The Dark”, a book about many of the DOJ and Treasury employees who contributed to this investigation, describes Prof. Sara Meiklejohn’s early work as the foundation for Chainalysis’ tools, and her work has been cited by government experts.
- “Gronager, affable as always, told Meiklejohn that his tiny company, Chainalysis, was looking for talent and asked her if she might be interested in becoming the “head of something or other,” as she remembers it. He showed her a demo of Reactor; she was impressed with how Gronager had managed to refine and scale up her group’s techniques, assembling a vast collection of known Bitcoin clusters and integrating several of the ideas she’d first demonstrated into a powerful and highly responsive tool.” Tracers in the Dark at p. 402.

EVALUATING CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS

Meiklejohn in 2022 presenting the paper offered into disclosure by Ms. Bisbee: "[In a description of clustering heuristics] The heuristic as I've just described it is horribly unsafe. You would like collapse probably everything together at this point in bitcoin's evolution, this on its own is extremely unsafe, you can make a lot of modifications and adjustments…"

"[about her new heuristic described in the 2022 paper disclosed by the government's expert] it wasn't possible to run our heuristic in 2013….

"If you get that wrong, it's like a huge clustering error…that one time deposit address that you might have mistakenly mislabeled as a change address might get used with like 50 other addresses at the same time."

See Sarah Meiklejohn, De-Anonymization in Bitcoin with Sarah Meiklejohn | a16z crypto research talks, https://youtu.be/slZgOwXt2jM.

EVALUATING CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS

- Blockchain Tracing Tools Useful For Leads To Focus Investigations, But Real-World Evidence Required To Attribute Ownership of Illicit Funds: just a core accepted position in every crypto training I have received as a CPA/CFF, also happens to have been written about by attorneys who have authored leading work in crypto forensics who I previously cited in my own book on crypto forensics and privacy before joining this case:
- "In addition to using blockchain analysis for pure lead purposes, it can also be used in search and seizure warrants. Similar to instances where blockchain analysis leads to a subpoena or a Financial Crimes Enforcement Network database query at the initiation of an investigation, its use in warrants is often an intermediate step used to justify searching a subject's residence, digital devices, or other location- ***however with the understanding that the fruits of that search*** (such as drug paraphernalia, child pornography, incriminating text messages, etc.) ***will provide the primary evidence of the subject's guilt at trial, rather than the blockchain analysis***."
- See C. Alden Pelker, Christopher B. Brown, & Richard M. Tucker, Using Blockchain Analysis From Investigation to Trial , 66 DOJ Journal of Federal Law and Practice May 2021, available at https://www.justice.gov/media/1169626/dl?inline.

EVALUATING CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS

- Emphasis on this portion from the article quoted in the last slide:
- **"*however with the understanding that the fruits of that search*** (such as drug paraphernalia, child pornography, incriminating text messages, etc.) ***will provide the primary evidence of the subject's guilt at trial, rather than the blockchain analysis***."
- See C. Alden Pelker, Christopher B. Brown, & Richard M. Tucker, Using Blockchain Analysis From Investigation to Trial , 66 DOJ Journal of Federal Law and Practice May 2021, available at https://www.justice.gov/media/1169626/dl?inline.
- To Be Clear: I HAVE FOUND NO SUCH EVIDENCE PRESENTED IN THIS CASE LINKING MR. STERLINGOV TO THE PURCHASE OF THE BITCOIN FOG DOMAIN OR TO BTC FOG FEE PROCEEDS

EVALUATING CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS

- Coinjoin and payjoin activity confounds heuristics behind Chainalysis tracing

- The first equal-amount coinjoins that can be observed on-chain were likely 2013 and equal-amount coinjoins became more common in 2014/2015 (dark wallet + joinmarket).

EVALUATING CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS

- Payjoin activity, which was possible and highlighted even earlier in Bitcoin's history than equal-amount coinjoins, more strongly confounds heuristics behind Chainalysis tracing
- Payjoins were used in the wild before equal-amount coinjoins. A feature introduced by MTGox facilitated payjoins out of that platform early in its history. Meiklejon has indicated in prior literature that one of the assumptions behind her description of exchange data as "ground truth" is that exchanges don't allow coinjoins or payjoins, but that wasn't true for Mt. Gox.
- If Mt Gox errors from this phenomenon have been controlled for within the Chainalysis black box, we need to know precisely how and have an opportunity to test the source code there.

EVALUATING CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS

- Are the Mt. Gox records reliable for purposes of a financial forensic examination or analysis?
- Karpeles description of state of records on Up Only podcast **suggests Mt Gox not credible**
- Evidence Mt. Gox Hacked repeatedly **suggests Mt Gox not credible**
- Prior Conviction of Karpeles **suggests Mt Gox not credible**
- Hacker Behavior Pattern in Using Login Credentials for Illicit Activity **suggests Mt Gox not credible**
- Mt. Gox "coinjoin mess" issue is problem for post-Mt Gox forensics. We need to see every detail in how Chainalysis attempted to control for it and any "dry holes" or abandoned investigative focus in their efforts to ensure no bias was present. **suggests Mt Gox not credible**
- **Determination: Mt. Gox Records Not Reliable For Crypto Attribution**

RESULTS FOR CLAIM II: CAN BLOCKCHAIN TRACING ATTRIBUTE PROPERTY OWNERSHIP IN ILLICIT FUNDS?

- **No, it is insufficiently reliable for that purpose.**
- Blockchain tracing can be used to generate leads in investigations. But only ground truth data like possession of private keys, possession of server logs, or reliable evidence from a "KYC" platform can attribute illicit crypto ownership to an individual
- No such evidence exists in this case to tie Mr. Sterlingov to operation of Bitcoin Fog
- The only potential ground truth evidence was Mt. Gox, but it is both unreliable, and even if reliable does not solve problems with property attribution following transfers between Mt. Gox and Liberty Reserve.

CLAIM III: WAS THE GOVERNMENT'S DESCRIPTION OF "BETA TRANSACTIONS" ACCURATE

- Legitimate alternative explanation in that early bitcoin paper wallet users and laptop wallet users were highly concerned about wallet security and reliability, and thus conducted test transactions for new wallet use and for onboarding new users.
- Subsequent transfers to Bitcoin Fog reflect that Bitcoin Fog was known on Bitcointalk forum as a new privacy tool
- **Professional Determination: Unclear and Unsubstantiated Allegation**

FINANCIAL FORENSIC FINDINGS:

- Through Application of the Standards of Forensic Accounting and Fraud Examination (or generally, the standards of financial forensics):
- **My professional findings are that there is:**
- No evidence at all presented by the government that Mr. Sterlingov received fees from Bitcoin Fog
- No reliable evidence linking Mr. Sterlingov to the purchase of the bitcoinfog.com clearnet domain
- No reliable evidence that what the government describes as "beta test" transactions were not harmless bitcoin wallet reliability testing