**UNITED STATES DISTRICT COURT**
**DISTRICT OF COLUMBIA**

| | |
|---|---|
| UNITED STATES OF AMERICA<br><br>Plaintiff,<br>v.<br><br>ROMAN STERLINGOV<br><br>Defendant. | **No. 21-cr-399 (RDM)** |

**DEFENDANT'S NOTICE OF INTENT TO PRESENT EXPERT TESTIMONY**

Defendant Roman Sterlingov by and through counsel, and under Fed. R. Evid. 702, 703, and 705, and Federal Rule of Criminal Procedure 16, hereby provides notice of his intent to introduce expert testimony at the June 16 & 23, 2023, hearings on the outstanding Motions in Limine and *Daubert* challenges, as well as at trial. The witnesses listed below possess special skills and knowledge that will assist the Court and Jury in understanding the evidence in this case. The Defense hereby provides notice of the anticipated testimony of the expert witnesses listed below. These witnesses' testimony should be considered expert testimony under Rule 702. Each expert witnesses' curriculum vitae has been sent to the Court and the Government via email.

As the Defense's investigation and review of the Government's discovery proceeds, we will supplement these disclosures as necessary.

**INTRODUCTION**

The Government charges Mr. Sterlingov with Conspiracy to Launder Monetary Instruments, in violation of 18 U.S.C. § 1956(h); Money Laundering, in violation of 18 U.S.C. § 1956(a)(3)(A), (B); Operating an Unlicensed Money Transmitting Business and Aiding and

Abetting, in violation of 18 U.S.C. § 1960(a) and 18 U.S.C. § 2; and Money Transmission Without a License, in violation of D.C. Code § 26-1023(c).

There is no evidence of Roman Sterlingov ever operating Bitcoin Fog. What forensics evidence the Government has turns on new and standardless black-box blockchain forensic software implementing unscientific, non-peer-reviewed heuristic algorithms to trace Bitcoin transactions. Using speculative digital forensics, the Government indulges in confirmation bias making inaccurate I.P. address attributions, blockchain clustering assertions, and conclusory assumptions about The Onion Routing Network (TOR Network), financial accounting forensics, encryption, mathematics, and computer science that are not within the common knowledge of the average juror. The lack of forensic evidence showing Mr. Sterlingov operating Bitcoin Fog, its complete absence from any of his seized electronic devices, storage devices, notes, and diaries goes directly to the integrity of the Government's prosecution. This is the first real test of Chainalysis Inc.'s black-box blockchain forensics. It is the first time the Government's forensics in a blockchain case like this face adversarial testing at trial. The testimony of these experts is crucial to demonstrating the Government's flawed, biased forensics, and glaring omissions.

Federal Rule of Evidence 702 governs the admissibility of expert testimony. Expert testimony is appropriate if specialized knowledge will assist the jury "to understand the evidence or to determine a fact in issue." *United States v. Eiland*, No. 04-379 RCL, 2006 WL 2844921, at *5 (D.D.C. Oct. 2, 2006) *aff'd*, 738 F.3d 338 (D.C. Cir. 2013).

A witness qualified as an expert by knowledge, skill, experience, training, or education may testify thereto in the form of an opinion or otherwise, if "(1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and

(3) the witness has applied the principles and methods reliably to the facts of the case." *Id*. (citing Fed. R. Evid. 702).

In order to qualify as an expert and offer expert testimony, a witness must possess "knowledge, skill, experience, training, or education" on the subject about which he is testifying. Fed. R. Evid. 702.

On December 1, 2022, the latest amendment to Fed. R. Crim. Pro. 16 went into effect. This case commences prior to the adoption of the revised rule; thus, this Court should hold that the prior version of Fed R. Crim. Pro. 16 applies. Justice Roberts, in submitting the amended rule to Congress, advises that the Amendment "shall govern in all proceedings in criminal cases thereafter commenced and, insofar as just and practicable, all proceedings then pending."[1] It is not just and practicable to apply the amended rule this late into the case because the Defense began working on expert testimony before this Amendment came into effect. The Firm made trial strategy decisions under the rubric of the then current version of Rule 16. To the extent Defendant's request for a continuance plays into the Court's consideration in this matter, the Government's seizure of Mr. Sterlingov's assets forced the Defense to request a continuance to search for funding for the case, and volunteers to staff it. Without funds to properly staff the case, the transaction time for everything increases.

Should the Court hold that the latest Amendment applies, the Defense will supplement these disclosures as necessary.

**EXPERT WITNESSES**

The Defense intends to call the following expert witnesses. Their qualifications, along with review and analysis of relevant records, reports, facts, and evidence, set forth the bases for

[1] Fed R. Crim. Pro. 16 Submission Letter, from Justice John Roberts to Hon. Nancy Pelosi and Hon. Kamala Harris, April 11, 2022.

their testimony. The Defense will update this disclosure as necessary for the June hearings and trial, and will provide the Government with any expert reports as warranted.

**A. Dr. Francisco Xavier Cabañas**

Mr. Sterlingov intends to call **DR. FRANCISCO CABAÑAS** ("Dr. Cabañas") as an expert witness. His qualifications, along with review and analysis of relevant records, reports, facts, and evidence set forth the basis for his expected testimony.

Dr. Cabañas' testimony is based on his review of discovery in this case, and his depth of experience in digital currencies, blockchain forensics and statistical analysis. Since 2016, he has been a core team member of Monero's development organization. He is a key contributor to the European Union's Public Consultation on Preventing Money Laundering and Terrorism Financing. He has 45 years of experience as a computer and network administrator and has a wide range of experience with data analysis and technologies.

Since 2020, Dr. Cabañas has been a contributor with the Monero Policy Working Group through which he has advanced the privacy protocols of the Monero cryptocurrency and developed scaling technologies to expand the Monero network.

Dr. Cabañas has spoken at many panels and conferences around the world advocating for privacy in cryptocurrency and has shared his research with privacy interest groups around the globe.

Dr. Cabañas holds a Ph.D. in Physics, a M.Sc. in Physics, and a B.Sc. Honors in Physics and Mathematics from the University of British Columbia. He has over 20 years of experience in the fields of experimental physics, physical chemistry, and radio astronomy where he specialized in mathematical analysis of random errors (or noise) and systematic errors (bias) in statistics.

At the June 16, 2023 hearing on Motions in Limine and *Daubert* challenges, as well as at trial, the Defense expects Dr. Cabañas to testify regarding the following:

1. The Defense expects Dr. Cabañas to testify to the importance of differentiating between proprietary closed source blockchain surveillance software like Chainalysis Reactor (the Government's main forensic vendor in this case) and public, open-source tracing on the public blockchain by forensic software like OXT and the like.
    a. He will explain how blockchain surveillance, unlike open-source transaction analysis, makes assumptions and guesses regarding the ownership of anonymous public keys.
    b. He will explain how the opaque methodologies and lack of peer-review make it impossible to scientifically verify Chainalysis's and the Government's findings.
2. The Defense expects Dr. Cabañas to testify to the scientific illegitimacy of the blockchain forensics used in this case.
    a. He will explain that the Government's forensic evidence does not meet scientific standards and cannot be relied upon.
    b. He will explain the statistical and mathematical limitations of the heuristic blockchain tracing methodologies at issue here.
    c. He will explain how blockchain surveillance software like Chainalysis Reactor cannot scale with the rise in global cryptocurrency activity and produces inaccurate tracing.

3. The Defense expects Dr. Cabañas to testify to the relative bias and systemic errors prevalent in blockchain surveillance tools including Chainalysis Reactor.
    a. He will explain the scope of illicit virtual asset transfers, as documented by the Financial Action Task Force studies. (*See* Ex. B).
    b. He will explain how different blockchain forensic tracing softwares make contradictory cluster attributions for identical addresses.
    c. He will explain how this variability introduces a high level of arbitrariness into forensic conclusions.
    d. He will explain that the percentage of transactions implicated in illegal activity is as low as 0.5% and as high as 12.7% depending on which blockchain surveillance company conducts the analysis.
4. The Defense expects Dr. Cabañas to testify to the Defense's blockchain tracing of the key Government tracings in this case.
    a. He will explain how tracing via open source OXT blockchain forensic software, along with other forensic tracing software, fails to verify the Government's forensic blockchain tracing.
5. The Defense expects Dr. Cabañas to testify that it is possible to transfer Bitcoin without leaving any trace on the blockchain, and that this possibility makes attribution of blockchain activity to a specific individual unverifiable absent corroborating evidence.
    a. He will explain how public and private keys work on the blockchain.
    b. He will explain how it is impossible to know for certain who, if anyone, exercises direct control over the keys.

c. He will explain how digital currency like Bitcoin can be transferred off chain.

d. He will explain the problems that off-chain transfers of cryptocurrency cause for blockchain tracing forensics.

6. The Defense expects Dr. Cabañas to testify that the tracing of the purported Bitcoin Fog beta transactions as alleged by the Government is not indicative of Mr. Sterlingov being the operator of Bitcoin Fog.

a. He will explain that there are multiple possible results for the Government's and Chainalysis's forensics attributing the purported beta transactions to Mr. Sterlingov.

b. He will explain that the transactions identified by the Government and Chainalysis as Bitcoin Fog beta transactions are not consistent with beta transactions.

c. He will explain that the Bitcoin network allows for off-chain beta transactions that are used to test networks without sending real Bitcoin through the public blockchain.

7. The Defense expects Dr. Cabañas to testify to FTX blockchain compliance vendor Chainalysis's failure to identify illegal activity at FTX.

a. He will explain that Chainalysis had an oversight role with FTX but failed to identify any criminality occurring at FTX.

b. He will explain how other tracing firms also had oversight of FTX's operations and failed to identify any criminal conduct.

8. The Defense expects Dr. Cabañas to testify to the statistical difficulties with calibrating blockchain forensics.
    a. He will explain the mathematical difficulties of properly calibrating the false positive rate of the Government's digital forensics.
9. The Defense expects Dr. Cabañas to testify to the mathematical issues of the different probabilistic blockchain heuristic methodologies used for tracing.
    a. He will explain the limitations of Chainalysis' black-box surveillance techniques, and the utility of forensic transparency in opposition to Chainalysis' methodologies.
10. The Defense expects Dr. Cabañas to testify in rebuttal to the government's expert testimony.
    a. The content of Dr. Cabañas' rebuttal testimony is contingent on the substance of testimony from the witnesses produced by the Government in the Hearings and at trial.

**B. Dr. Itiel Dror**

Mr. Sterlingov intends to call **DR. ITIEL DROR** ("Dr. Dror") as an expert witness. His qualifications, along with review and analysis of relevant records, reports, facts, and evidence set forth the basis for his expected testimony.

Dr. Dror's testimony is based on his review of discovery in this case, and his academic and professional experiences. Dr. Dror is a Principal Consultant and Researcher with Cognitive Consultants International ("CCI-HQ") through which he provides research, training, and consultancy services to organizations around the world concentrating on minimizing bias in

expert decision making and investigations. Dr. Dror holds a Ph.D. and a master's degree from Harvard University in Psychology.[2]

Dr. Dror trained the forensic digital experts at the Serious Fraud Office (SFO) in the United Kingdom (the U.K. governmental body investigating serious fraud, where digital evidence is critical). He was commissioned by the United States Attorney's Office in this District for a *Daubert* Hearing. Dr. Dror trains forensic experts at top investigative agencies all over the world, including the United States, about bias in digital and other forensic domains. He has been commissioned to train forensic experts at the FBI, NYPD, LAPD, and many other agencies, on how to minimize biases in their investigations. He has been invited by the National Institute of Justice and the Department of Justice, as well as many other agencies, to deliver keynote presentations. Recently, the Attorney General of the State of Maryland has asked Dr. Dror to be part of the design team for the review of potential bias in forensic decisions made about deaths of people while in police custody.

Dr. Dror has published over 150 articles which have been cited over 10,000 times, with an h-index of 55 (i.e., 55 articles that are cited over 55 times), these include articles with over 600 citations, and over 30 articles with over 100 citations. Many of the articles appear on the most viewed and most cited lists of several journals. Furthermore, his articles and research has been cited in various court cases,[3] as well as by the U.S. National Commission on Forensic Science, the National Academy of Science report on forensic science, and the President's Council of Advisors on Science and Technology's report on forensic science.[4]

---

[2] *See* Ex. C.
[3] *See e.g. Regina v. Dlugosz, Pickering, and MDS* (2013) (United Kingdom Court of Appeal); *Commonwealth vs. Gambora* (2012) (Supreme Court of Massachusetts).
[4] (*See* Ex. D-F).

Dr. Dror has been an Associate Editor and on the Board of Editors for multiple journals, including *Forensic Science International: Mind and Law*, *Science & Justice*, *Journal of Experimental Psychology: Applied*, *Journal of Applied Memory & Cognition*, and *Pragmatics & Cognition*.

Top scientific journals such as *Science* and *Nature*, as well as media outlets like *The Economist*, *the New York Times*, *the Guardian* and *the London Times* cover Dr. Dror's work and research findings on how bias impacts forensic science decisions, and ways to minimize such biases.[5]

At the June 23, 2023 hearing on Motions in Limine and *Daubert* challenges, as well as at trial, the Defense expects Dr. Dror to testify regarding the following:

1. The Defense expects Dr. Dror to testify generally about cognitive bias in forensic science, and particularly about the role of confirmation and other biases in digital forensic investigations.
    a. He will explain the concept of cognitive bias (in contrast to the everyday notion of intentional and discriminatory biases).
    b. He will explain the current state of the research and scientific standards related to cognitive bias in relation to forensic decisions.
    c. He will explain how the brain processes decisions, and how architecture constraints give rise to biases.
    d. He will explain the eight sources of cognitive and human error that exist specifically within the framework of digital forensics, and the six fallacies about bias.

[5] (*See* Ex. G).

2. The Defense expects Dr. Dror to testify about confirmation and other biases in digital forensics.
    a. He will explain confirmation and other biases that impact hard working and dedicated forensic experts.
    b. He will explain how confirmation and other biases taint an investigation.
    c. He will explain evidence of confirmation bias from the Government's discovery.
    d. He will explain how escalation of commitment can lead to inaccurate conclusions contrary to the evidence.
3. The Defense expects Dr. Dror to testify to the cognitive and human factors in digital forensics.
    a. He will explain how miscarriages of justice and misleading evidence highlight human error as an issue within forensic science.
    b. He will explain the issues and the fertile ground for biases created by the lack of objective standards in blockchain forensics.
4. The Defense expects Dr. Dror to testify in rebuttal to the government's expert testimony.
    a. The content of Dr. Dror's rebuttal testimony is contingent on the substance of testimony from the witnesses produced by the Government in the Hearings and at trial.

**C. Jeffrey Fischbach**

Mr. Sterlingov intends to call **JEFFREY FISCHBACH** ("Mr. Fischbach") as an expert witness. His qualifications, along with review and analysis of relevant records, reports, facts, and evidence set forth the basis for his expected testimony.

Mr. Fischbach's testimony is based on his review of discovery in this case, and his experience as a Board Recognized Forensic Examiner specializing in computer forensics, information communication, stored data, and electronic location technologies. Mr. Fischbach is an expert in these fields for over twenty-five years and has consulted on, and testified in, municipal, federal, and military court, both domestic and foreign, in dozens of cases involving computer forensics and digital evidence. Mr. Fischbach routinely lectures and provides training in his areas of expertise to civilian attorneys, law enforcement, and judges throughout North America.

Mr. Fischbach is the founder and President of SecondWave, Inc., a technology consulting firm specializing in forensic technology, evidence preservation, and authentication. Mr. Fischbach has expert-level knowledge of Windows, MacOS, Linux, iOS and Android operating systems. He has qualified in numerous courts as a computer, internet, cellular and satellite expert. He has previously been granted national security clearance by the United States Department of Justice.

Mr. Fischbach will explain the forensically unsound techniques used in this case including the chain of custody and authenticity issues inherent in the Government's digital evidence and forensics. Mr. Fischbach will show that Chainalysis's work does not meet scientific forensic standards, and that any work done by them in this case cannot be relied upon at trial.

At the June 16 and 23, 2023 hearings on Motions in Limine and *Daubert* challenges, as well as at trial, the Defense expects Mr. Fischbach to testify regarding the following:

1. The Defense expects Mr. Fischbach to testify that the Government has failed to produce any sound forensic evidence that demonstrates Mr. Sterlingov created or operated the Bitcoin Fog onion bitcoin mixing site.

2. The Defense expects Mr. Fischbach to testify to the fact that the chain of custody of the Mt. Gox data is unreliable, cannot be authenticated as a business record, and should be excluded from evidence.
    a. He will explain how the Mt. Gox data was corrupted by the 2014 Mt. Gox hack, and that these records do not reflect the true transactions that took place on the Mt. Gox platform.
    b. He will explain how the derivative Mt. Gox data produced by the Government cannot be authenticated because there are no original server logs, or any original native data.
3. The Defense expects Mr. Fischbach to testify that using IP addresses as personal identifiers is forensically unsound.
    a. He will explain that thousands of people can share the same IP address through VPNs, proxy servers, IP address spoofing, use of common WiFi routers, IP address high jacking and the like.
    b. He will explain why IP address matches are an unreliable means of identifying an individual, to which he has previously provided testimony as an expert witness.
    c. He will explain that courts do not accept IP address matches as personally identifying information.
4. The Defense expects Mr. Fischbach to testify to the review of the public blockchain.
    a. He will explain that the clustering methodologies put forth by the Government and Chainalysis can result in multiple different outcomes,

and that any trace to Mr. Sterlingov is subjective, based on guessing, and is not determinative or based on sound forensic techniques.

b. Using OXT, an open source blockchain tracing firm that closed source Chainalysis sought to buy, he will explain that Chainalysis's results are based on selective input datasets that do not amount to competent or scientific forensics.

5. The Defense expects Mr. Fischbach to testify to the application of blockchain tracing in digital forensics.

a. He will explain the subjectivity and inherent problems in the use of probabilistic heuristic algorithms in the source code for software like Chainalysis Reactor.

b. He will explain how input datasets are subjective, not objective, and lead to inaccurate, unverifiable conclusions.

c. He will explain the difference between closed source and open source blockchain tracing software, contrasting the Government's use of closed source, proprietary Chainalysis Reactor with the Defense's use of public, open source OXT tracing software.

6. The Defense expects Mr. Fischbach to testify to the Defense's blockchain tracing of the key Government tracings in this case.

a. He will explain how tracing via open source OXT blockchain forensic software, along with other forensic tracing software, fails to verify the Government's forensic blockchain tracing.

7. The Defense expects Mr. Fischbach to testify that the Government's alleged tracing of the purported Bitcoin Fog beta transactions is not indicative of beta testing of a new .onion site.
    a. He will explain that there are multiple possible results for the Government's and Chainalysis's forensics attributing the purported beta transactions to Mr. Sterlingov.
    b. He will explain that the transactions identified by the Government and Chainalysis as Bitcoin Fog beta transactions do not appear to be beta transactions.
    c. He will explain that the Bitcoin network allows for off-chain beta transactions that are used to test networks without sending real Bitcoin through the public blockchain.
8. The Defense expects Mr. Fischbach to testify to the fact that the Government's and Chainalysis's forensic methodologies fail basic forensic standards.
    a. He will explain the application of the scientific method in the field of digital forensics.
9. Mr. Fischbach will testify as to what is involved in operating a .onion site and custodial mixer like Bitcoin Fog.
    a. He will explain the need for constant maintenance of the site.
    b. He will explain the high level of information security required for a .onion site like Bitcoin Fog that is subject to continual hacking attempts.
    c. He will discuss the staffing requirements to run an enterprise like Bitcoin Fog.

10. The Defense expects Mr. Fischbach to testify to the fact that the Government's forensic conclusions are based on forensics that have not been peer-reviewed.
    a. He will explain the process of peer-review.
    b. He will explain the difference between a whitepaper and scientifically accepted peer-review.
11. The Defense expects Mr. Fischbach to testify to the methods of buying, selling, mining, and valuing cryptocurrency.
12. The Defense expects Mr. Fischbach to testify to the Chainalysis contracting process.
    a. He will explain that there appear to be no attempts by the U.S. Government to evaluate the efficacy of Chainalysis' blockchain tracing methodologies.
    b. He will explain how the government appears not to have followed general standards in contracting procedures when signing contracts with Chainalysis.
13. The Defense expects Mr. Fischbach to testify to the use and application of the hardware Mr. Sterlingov had in his possession at the time of his arrest.
    a. He may explain how the hardware Mr. Sterlingov was travelling with when he was arrested is common in the computer world.
    b. He will identify the purpose and function of each device Mr. Sterlingov had in his possession at the time of his arrest.
14. The Defense expects Mr. Fischbach to testify in rebuttal to the government's expert testimony.

a. The content of Mr. Fischbach's rebuttal testimony is contingent on the substance of testimony from the witnesses produced by the Government in the Hearings and at trial.

**D. Jonathan Scott**

Mr. Sterlingov intends to call **JONATHAN SCOTT** ("Mr. Scott") as an expert witness. His qualifications, along with review and analysis of relevant records, reports, facts, and evidence set forth the basis for his expected testimony.

Mr. Scott's testimony is rooted in his extensive theoretical and practical expertise in computer science, which he has gained through his training, review of the discovery materials, and certification as a cryptocurrency auditor by the Blockchain Counsel. Currently, Mr. Scott holds multiple roles in the field of blockchain technology: he serves as a blockchain forensics examiner and smart contract auditor at Redlion, LLC; a senior blockchain engineer at WeGrow LLC; and a mobile forensic examiner, CNO developer, and ransomware analyst for a United States government agency. Additionally, Mr. Scott was employed by The CELO Foundation, where he was specifically recruited to contribute to the CELO token platform. In this capacity, he was responsible for strengthening the platform's infrastructure and conducting meticulous blockchain forensics analysis on wallets associated with DeFi projects seeking partnerships with CELO.

With a background in computer science and digital forensics, Mr. Scott possesses extensive knowledge of blockchain technology. He is well-versed in diverse tools used for blockchain forensic tracing and will discuss his efforts to replicate the Government's tracing methods for crucial aspects of their case.

In 2021, hackerone.com ranked Mr. Scott as the top white-hat hacker in the United States. His exceptional abilities led him to discover and report over 740 vulnerabilities, all of which have been resolved since. In 2022, he was publicly acknowledged and rewarded for demonstrating how the highly secure SecuX Crypto Hardware wallet and the supposedly impenetrable Ellipal Tital Crypto Hardware wallet could be breached. Additionally, Mr. Scott consistently demonstrates his expertise by earning CVE credentials for successfully exploiting LG Android OS mobile devices with the goal of making them more secure. He routinely undertakes digital forensic assignments for various US and international government agencies.

Mr. Scott is currently completing his doctorate in computer science, specializing in digital forensics and malware analysis. He has a Master of Science degree in Computer Science from Colorado Technical University, where he concentrated on cybersecurity engineering. He obtained a bachelor's degree in Philosophy from the University of Tennessee, Knoxville.

At the June 16 and 23, 2023 hearings on Motions in Limine and *Daubert* challenges, as well as at trial, the Defense expects Mr. Scott to testify regarding the following:

1. The Defense expects Mr. Scott to testify to the Defense's blockchain tracing of the key Government tracings in this case.
    a. He will explain how tracing via open source OXT blockchain forensic software, along with other forensic tracing software, fails to verify the Government's forensic blockchain tracing.
2. The Defense expects Mr. Scott to testify to the scientific illegitimacy of Chainalysis's and other Government forensic vendors' work on this case.

a. He will explain the scientific process, how technical analyses are peer-reviewed, and how the Government's and Chainalysis's black-box forensics fail to meet international scientific standards.

3. The Defense expects Mr. Scott to testify about Bitcoin and computer culture generally.
    a. He will explain the proliferation of Bitcoin meetups like the ones Mr. Sterlingov went to.
    b. He will explain the privacy concerns that cryptocurrency users have, and why mixing is integral to personal privacy.
    c. He will explain the benefits of using mixing services.
4. The Defense expects Mr. Scott to testify to the use and application of the hardware Mr. Sterlingov had in his possession at the time of his arrest.
    a. He will explain how the hardware Mr. Sterlingov was travelling with when he was arrested is common in the computer world.
    b. He will identify the purpose and function of each device Mr. Sterlingov had in his possession at the time of his arrest.
5. The Defense expects Mr. Scott to testify to Chainalysis's and the Government's flawed forensic examination of the alleged beta transactions.
    a. He will explain why Chainalysis's and the Government's investigation was flawed from its outset.
    b. He will explain the nature of the blockchain and how beta testing is conducted.
6. Mr. Scott will testify regarding Mr. Sterlingov's Kraken account.

a. He will explain that the Government's allegation that Mr. Sterlingov's Kraken account received service fees from Bitcoin Fog is speculative and forensically unsound.

b. He will explain how the deposits, withdrawals, and trades are inconsistent with the Government's service fee payment theory.

c. He will explain the different ways to hold cryptocurrency and the differences between exchanges and wallets.

d. He will explain why no sophisticated cybercriminal or money launderer would deposit illicit funds into a Know Your Customer ("KYC") cryptocurrency exchange account like Kraken.

e. He will explain the difference between custodial and non-custodial wallets and exchanges.

7. The Defense expects Mr. Scott to testify that the tracing of the purported Bitcoin Fog beta transactions is not indicative of Mr. Sterlingov being the operator of Bitcoin Fog.

a. He will explain that there are multiple possible results for the Government's and Chainalysis's forensics attributing the purported beta transactions to Mr. Sterlingov.

b. He will explain that the transactions identified by the Government and Chainalysis as Bitcoin Fog beta transactions do not appear to be beta transactions.

c. He will explain that the Bitcoin network allows for off-chain beta transactions that are used to test networks without sending real Bitcoin through the public blockchain.

8. The Defense expects Mr. Scott to testify to the inauthenticity and scientific invalidity of the Mt. Gox records.

   a. He will explain how hacks can distort data.

   b. He will explain how the Mt. Gox data has been distorted.

   c. He will explain why the Mt. Gox data cannot be relied upon to derive accurate results.

9. The Defense expects Mr. Scott to testify to Chainalysis's flawed hypothesis that the DNS registration for the Clearnet site www.bitcoinfog.com implicates Mr. Sterlingov.

   a. He will explain how the Government's and Chainalysis's tracing analysis is arbitrary and unverifiable.

   b. He will explain how DNS registrations work, how they need to be renewed, and how the DNS identified in the Criminal Complaint was renewed.

   c. He will explain why the heuristic clustering methodologies employed by the Government and Chainalysis are subject to a significant amount of statistical bias.

10. Mr. Scott will testify as to what is involved in operating a .onion site and custodial mixer like Bitcoin Fog.

    a. He will explain the need for constant maintenance of the site.

b. He will explain the high level of information security required for a .onion site like Bitcoin Fog that is subject to continual hacking attempts.

c. He will discuss the staffing requirements to run an enterprise like Bitcoin Fog.

11. The Defense expects Mr. Scott to testify as to the contracting procedures for federal government agencies.

a. He will explain the disclosure requirements for federal contracts.

b. He will explain how the contracts between DOJ and Chainalysis fail to meet the minimum standards set out by law.

c. He willexplain how the development of Excygent, LLC and its subsequent sale to Chainalysis fails to meet the minimum disclosure requirements set out by law.

11. The Defense expects Mr. Scott to testify in rebuttal to the government's expert testimony.

a. The content of Mr. Scott's rebuttal testimony is contingent on the substance of testimony from the witnesses produced by the Government in the Hearings and at trial.

**E. J.W. Verret**

Mr. Sterlingov intends to call **JOHN WALLACE "J.W." VERRET JD, MPP, CPA/CFF, CFE, CVA** ("Mr. Verret") as an expert witness. His qualifications, along with review and analysis of relevant records, reports, facts, and evidence set forth the basis for his expected testimony.

Mr. Verret is an expert in crypto forensics, financial privacy, forensic accounting, financial forensics, banking regulation, and anti-money laundering. An Associate Professor of

Law at the George Mason University Antonin Scalia School of Law, he teaches legal courses in forensic accounting, corporate law, securities law, and banking law/AML. He is a practicing attorney and works in internal accounting investigations and financial regulatory enforcement, the latter with an emphasis on digital currency projects.

Mr. Verret was a Visiting Professor at Stanford Law School, where he taught a course in financial regulation. He has a J.D. from Harvard Law School, a Masters in Public Policy from the Harvard Kennedy School with an emphasis in financial regulation, and a B.S. from Louisiana State University in Accounting. He holds a certificate from the Wharton Business School in the Economics of Blockchain. He is a Certified Public Accountant in the state of Virginia, is Certified in Financial Forensics (CFF) by the AICPA, is a Certified Fraud Examiner (CFE) and a Certified Valuation Analyst (CVA).

Mr. Verret serves on the Financial Accounting Standards Advisory Council, a group that advises the Financial Accounting Standards Board on the development of Generally Accepted Accounting Standards (GAAP) and where he recently advised on the development of a new accounting standard for cryptocurrency reporting by public companies.

He currently serves on the board of directors of the Zcash Foundation, a non-profit that funds research into the zero-knowledge proof cryptography that underlies the privacy enhanced cryptocurrency Zcash and that other cryptocurrencies like Ethereum and Monero use to preserve user financial privacy. He is a columnist on cryptocurrency regulation and privacy for CoinTelegraph.

In 2013 he led the first briefing for members of Congress on the operation of Bitcoin. From 2013-2015, he was a Chief Economist and Senior Counsel for the U.S. House Financial Services Committee, where he works on congressional oversight of the Federal Reserve,

Treasury Department, AML/BSA compliance policy reform. While there he leads an investigation into insider trading at the Federal Reserve that results in the resignation of the President of the Federal Reserve Bank of Richmond. In his Senior Counsel role, he leads congressional oversight of the Treasury's Department's policy reforms to sanctions and money laundering and know your customer regulations regarding cryptocurrency. He has testified about financial and banking regulatory matters over a dozen times in the U.S. House of Representatives and the U.S. Senate. He is currently writing a book on cryptocurrency privacy and forensics for MIT Press.

Mr. Verret bases his expert opinions upon his extensive experience in cryptocurrency, financial privacy, financial forensic investigations, and law. His training and experience with federal regulators, combined with his proficiency and practice in cryptocurrency forensics, financial privacy, cryptocurrency, financial forensics, financial forensic investigations, professional accounting, banking regulations, anti-money laundering, and academia more than qualify him to present detailed expert opinion regarding this case.

At the June 16 and 23, 2023, hearings on Motions in Limine and *Daubert* challenges, as well as at trial, the Defense expects Mr. Verret to testify regarding the following:

1. Mr. Verret will testify regarding Mr. Sterlingov's Kraken account.
    a. He will explain that the Government's allegation that Mr. Sterlingov's Kraken account received service fees from Bitcoin Fog is speculative and forensically unsound.
    b. He will explain how the deposits, withdrawals, and trades are inconsistent with the Government's service fee payment theory.

c. He will explain the different ways to hold cryptocurrency and the differences between exchanges and wallets.

d. He will explain why no sophisticated cybercriminal or money launderer would deposit illicit funds into a Know Your Customer ("KYC") cryptocurrency exchange account like Kraken.

e. He will explain the difference between custodial and non-custodial wallets and exchanges.

2. Mr. Verret will testify to the transactions the government describes as "beta transactions".

a. He will explain that the early 2011 transfers through Bitcoin Fog that the Government misattributes to Mr. Sterlingov are not indicative of beta testing.

b. He will explain how the Government employs a simplistic view of what it describes as "beta transactions," how the transactions which the government describes with that phrase are unlikely to represent testing of a privacy mixer, and how there are multiple other reasonable explanations for what motivated those transactions.

3. Mr. Verret will testify regarding the Government's Mt. Gox data and Mt. Gox generally.

a. He will explain that the authenticity of the Mt. Gox data is in question.

b. He will explain the structure of Mt. Gox transactions, particularly how cryptocurrency and data was stored at Mt. Gox.

c. He will explain how Mt. Gox maintained a common cryptocurrency wallet for all Mt. Gox accounts and that when cryptocurrency was sent between Mt. Gox accounts, said transactions were done internally through a common Mt. Gox wallet and not registered on publicly viewable blockchains.

4. The Defense expects Mr. Verret to testify to the Defense's blockchain tracing of the key Government tracings in this case.

   a. He will explain how tracing via open source OXT blockchain forensic software, along with other forensic tracing software, fails to verify the Government's forensic blockchain tracing.

5. Mr. Verret will testify to the professional standards in financial forensics and forensic accounting investigations.

   a. He will explain why peer-review, verifiability, and reproducibility are integral aspects of financial forensics and forensic accounting investigations.

   b. He will explain how arbitrary assumptions laden with confirmation bias can impact the accuracy of financial forensics and forensic accounting investigations.

   c. He will explain how the heuristic blockchain forensics used by Chainalysis and the Government in this case cannot be relied upon to provide more than initial leads for the early stages of a financial forensic investigation and cannot alone determine whether a series of blockchain

transactions can be attributed to the same individual or to multiple individuals.

6. Mr. Verret will testify to the limited reliability of clustering and other heuristic techniques in cryptocurrency forensics.
    a. He will explain how the clustering methodologies and heuristic techniques applied in this investigation are often in error.
    b. He will explain how the clustering methodologies and heuristic techniques used in this investigation are probabilistic, not deterministic.
    c. He will discuss the different types of heuristics.
    d. He will explain how clustering is only applicable for generating leads, is far too speculative to prove anything specific, and cannot be relied upon to accurately identify a specific cryptocurrency user.
7. Mr. Verret will testify to the authenticity and attribution measures taken by investigators when conducting forensic investigations.
    a. He will explain how financial asset ownership attribution is determined in financial forensic investigations and will describe how the Government has failed to attribute any cryptocurrency proceeds of criminal transactions or laundered cryptocurrency assets to Mr. Sterlingov.
    b. He will explain how the Mt. Gox data cannot be authenticated because of chain of custody and manipulation issues, including the hack of the Mt. Gox servers, both digitally and physically.

c. He will explain the nature of the Mt. Gox hack, and why the Mt. Gox data produced by the government is inaccurate and does not meet Federal Rule of Evidence 901 or *Daubert* standards.

d. He will explain the dangers of using corrupted data in forensic investigations.

8. Mr. Verret will testify to the role input datasets play in blockchain tracing.

a. He will explain how input datasets are integral to cryptocurrency tracing investigations.

b. He will explain how review and analysis of the source code of Chainalysis Reactor and all digital blockchain forensic programs used in this case is necessary for Mr. Sterlingov to challenge his accusers and mount a complete defense.

c. He will explain how the corrupted Mt. Gox datasets result in inaccurate transaction traces.

9. Mr. Verret will testify to financial privacy in cryptocurrency transactions.

a. He will explain how people use custodial bitcoin mixers like Bitcoin Fog for privacy and security reasons.

b. He will explain why mixing is an integral part to maintaining privacy when using cryptocurrency.

c. He will explain why Bitcoin Fog and other privacy tools like coinjoins are common practice among legitimate and law abiding cryptocurrency users.

d. He will explain how standard cryptocurrency wallets are viewable by the public, and how if someone knows one's wallet address, they can see how much cryptocurrency is stored in that wallet.

e. He will explain that failure to employ privacy processes when dealing with cryptocurrency has made cryptocurrency users targets of hacks, kidnappings, robbery, lost bargaining/negotiation power, and the like.

f. He will explain how he teaches students to use privacy tools.

10. Mr. Verret will testify to FTX blockchain compliance vendor Chainalysis's failure to identify illegal activity at FTX.

a. He will explain that Chainalysis had an compliance oversight role with FTX, but failed to identify any criminality occurring at FTX.

b. He will explain how other tracing firms also had oversight of FTX's operations and failed to identify any criminal conduct.

11. Mr. Verret will testify to the best practices for financial privacy in cryptocurrency transactions.

a. He will explain the different privacy tools available to cryptocurrency users.

b. He will explain how mixing came about as a strategy for cryptocurrency users to secure their privacy interests.

12. Mr. Verret will testify to the culture of the cryptocurrency world and why users desire privacy.

13. Mr. Verret will testify as to what is involved in operating a .onion site and custodial mixer like Bitcoin Fog.

a. He will explain the need for constant maintenance of the site.

b. He will explain the high level of information security required for a .onion site like Bitcoin Fog that is subject to continual hacking attempts.

c. He will discuss the staffing requirements to run an enterprise like Bitcoin Fog.

14. Mr. Verret will testify as to how cryptocurrency transactions and holdings do not all appear on publicly viewable blockchain records.

a. He will explain the use of wallets and cold storage.

b. He will explain the nature of public and private keys in relation to Mr. Sterlingov's wallets and accounts.

c. He will explain how internal transfers within some platforms, like Mt. Gox, do not register on the blockchain.

15. Mr. Verret will also testify in rebuttal to the government's expert testimony.

a. The content of his rebuttal testimony is contingent on the substance of testimony from the witnesses produced by the Government in the Hearings and at trial.

**CONCLUSION**

The Defense submits that the expert testimony of the above witnesses will assist the jury and the Court in their understanding of the evidence in this case.

Dated: May 19, 2023
New York, New York

Respectfully submitted,

/s/ Tor Ekeland
Tor Ekeland (NYS Bar No. 4493631)
*Pro Hac Vice*
Tor Ekeland Law, PLLC
30 Wall Street, 8th Floor
New York, NY
t: (718) 737 - 7264
f: (718) 504 - 5417
tor@torekeland.com

/s/ Michael Hassard
Michael Hassard (NYS Bar No. 5824768)
*Pro Hac Vice*
Tor Ekeland Law, PLLC
30 Wall Street, 8th Floor
New York, NY
t: (718) 737 - 7264
f: (718) 504 - 5417
michael@torekeland.com

*Counsel for Defendant Roman Sterlingov*

**CERTIFICATE OF SERVICE**

I hereby certify that on the 19th day of May 2023, the forgoing document was filed with the Clerk of Court using the CM/ECF System. I also certify that a true and correct copy of the foregoing was sent to the following individuals via e-mail, and that experts' CVs were separately sent to the Court and the government via email:

s/ Tor Ekeland

U.S. Department of Justice
District of Columbia
555 Fourth St. N.W.
Washington, D.C. 20530

Catherine Pelker
Catherine.Pelker@usdoj.gov

Christopher Brown
Christopher.Brown6@usdoj.gov