Exhibit ‘C’

UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

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

SUMMARY OF QUALIFICATIONS AND EXPECTED TESTIMONY FOR 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 the 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. He will testify to the problems involved with the IP address attributions made by the Government, both in the produced discovery as well as the Government's expert reports. Mr. Fischbach will testify that the Government's unsound forensic and chain of custody techniques appear to have led them to mix evidence from an unrelated case with the evidence in Mr. Sterlingov's case, and how this compromises the integrity of the Government's conclusions.

At the July 19, 2023, hearing 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 that the public record demonstrates the Mt. Gox data is corrupt and unreliable, and should be excluded from evidence.
3. He will explain how Mark Karpeles's conviction for manipulation of the Mt. Gox data, inexplicable errors in the Mt. Gox data presented in discovery by the Government, as well as the numerous hacks of Mt. Gox render any reliance of the Mt. Gox data forensically unsound.

4. 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 that can be independently verified.
5. He will testify as to how the Japanese bankruptcy trustee cannot attest to the authenticity of the Mt. Gox data as this requires an individual with knowledge of the data's generation and chain of custody while it was at Mt. Gox, and before the trustee took possession of it.
6. The Defense expects Mr. Fischbach to testify that using IP addresses as personal identifiers is forensically unsound and how the Government has made its IP attributions in this case.
7. 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.
8. 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.
9. He will explain that courts generally do not accept IP address matches as personally identifying information.
10. The Defense expects Mr. Fischbach to testify to the fact that the Government's and Chainalysis's forensic methodologies fail basic forensic standards.
11. Mr. Fischbach will testify as to what is involved in operating a TOR network site and custodial mixer like Bitcoin Fog.
12. He will explain the need for constant maintenance of the site.

13. He will explain the high level of information security required for a TOR network site like Bitcoin Fog that is subject to continual hacking attempts.
14. He will discuss the staffing requirements to run an enterprise like Bitcoin Fog.
15. 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.
16. He will explain how the hardware Mr. Sterlingov was travelling with when he was arrested is common in the computer world, and what each piece of hardware is legitimately used for.
17. He will identify the purpose and function of each device Mr. Sterlingov had in his possession at the time of his arrest.
18. He will testify to the complete lack of any forensic evidence on any of Mr. Sterlingov's devices indicating that he ever operated Bitcoin Fog.
19. He will testify to the issues involved in Valerie Mazars de Mazarin's IP Overlap Analysis and related documentation produced by the Government.
20. He will testify to the issues in Valerie Mazars de Mazarin's Device Report and related documentation produced by the Government.
21. The Defense expects Mr. Fischbach to testify to Chainalysis's flawed hypothesis that the DNS registration for the Clearnet site www.bitcoinfog.com implicates Mr. Sterlingov.
22. He will explain how the Government's and Chainalysis's tracing analysis is arbitrary and unverifiable.
23. He will explain how DNS registrations work, how they need to be renewed, and how the DNS identified in the Criminal Complaint was renewed.

24. The Defense expects Mr. Fischbach to testify in rebuttal to the Government's expert testimony. In particular the expert testimony and reports of St. Jean and Mazarin.

    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.

Witness Attestation

I, Jeff Fischbach, have reviewed and approve the contents of this filing.

_____ _____

Jeff Fischbach Date