IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,
Plaintiff,

v. **Case No. 4:24-cr-00847-JSW**

DAVID CHEN,
Defendant.

DEFENDANT'S MOTION TO SUPPRESS DIGITAL EVIDENCE AND MEMORANDUM OF POINTS AND AUTHORITIES

TO THE HONORABLE JEFFREY S. WHITE, UNITED STATES DISTRICT JUDGE:

Defendant David Chen, through undersigned counsel, respectfully moves this Court pursuant to the Fourth Amendment to the United States Constitution and Federal Rule of Criminal Procedure 41(h) to suppress all digital evidence obtained through the search of his electronic devices and cloud storage accounts.

I. INTRODUCTION

This case involves allegations of computer fraud and abuse under 18 U.S.C. § 1030, stemming from alleged unauthorized access to SecureBank's customer database between January 2023 and March 2024. The government obtained digital evidence through a series of searches that violated Mr. Chen's Fourth Amendment rights due to:

1. **Overbroad search warrant scope** that exceeded constitutional particularity requirements
2. **Improper chain of custody** for digital forensic evidence
3. **Violation of attorney-client privilege** through examination of privileged communications
4. **Exceeding the scope** of the authorized search warrant

Mr. Chen seeks suppression of all evidence derived from these constitutional violations, which would effectively end the government's case.

II. STATEMENT OF FACTS

A. Background Investigation

On March 15, 2024, SecureBank reported to the FBI that their customer database had been accessed without authorization, resulting in the potential compromise of approximately 50,000 customer records containing personally identifiable information (PII). Initial forensic analysis by SecureBank's incident response team identified suspicious login activities from IP addresses traced to the defendant's residence.

B. Initial Search Warrant

On April 2, 2024, FBI agents obtained a search warrant from Magistrate Judge Maria Rodriguez authorizing the search and seizure of:

- All computers, laptops, tablets, and mobile devices at 1247 Oak Street, San Francisco, CA
- "Any and all data, information, or images evidencing violations of 18 U.S.C. § 1030"

C. Execution of Search Warrant

On April 5, 2024, FBI agents executed the warrant at defendant's residence, seizing:

- Two laptop computers (Dell XPS and MacBook Pro)
- One desktop computer system
- Three smartphones (iPhone 14, Samsung Galaxy S23, Google Pixel 7)
- External hard drives and USB storage devices
- Router and networking equipment

D. Digital Forensic Examination

The government's forensic examination, conducted by FBI Computer Analysis Response Team (CART), revealed:

- Evidence of sophisticated cybersecurity tools and penetration testing software
- Encrypted communications using Signal and ProtonMail
- Virtual private network (VPN) usage and Tor browser activity
- Cryptocurrency wallet addresses and transaction records

E. Discovery of Legal Privilege Issues

During forensic analysis, investigators accessed emails between Mr. Chen and his attorney regarding this investigation, as well as communications with other clients related to Mr. Chen's legitimate cybersecurity consulting business.

III. ARGUMENT

A. The Search Warrant Violated the Fourth Amendment's Particularity Requirement

1. Legal Standard

The Fourth Amendment requires that search warrants "particularly describe the place to be searched, and the persons or things to be seized." *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). This particularity requirement is especially critical in digital searches due to the vast amount of personal information stored on electronic devices. *Riley v. California*, 573 U.S. 373 (2014).

2. The Warrant Was Impermissibly Overbroad

The warrant's authorization to seize "any and all data, information, or images evidencing violations of 18 U.S.C. § 1030" fails constitutional particularity requirements. This language essentially authorized a general search of all digital content, violating the principle established in *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010).

The warrant should have been limited to:

- Specific time periods related to the alleged intrusion
- Particular file types or communications relevant to the investigation
- Defined search protocols to avoid over-seizure

3. Precedential Authority

In *United States v. Kik Interactive*, the court suppressed evidence where the warrant failed to adequately limit the scope of digital searches, noting that "the government cannot simply seize entire digital devices and sort out relevance later." Similar reasoning applies here, where the government's broad language permitted examination of privileged communications and unrelated business records.

B. Chain of Custody Violations Compromised Evidence Integrity

1. Forensic Imaging Irregularities

The government failed to maintain proper chain of custody during the forensic imaging process. FBI Agent Thompson's supplemental report indicates a two-hour gap in custody documentation when devices were transferred to the CART facility. During this period, the hash values used to verify data integrity were not recorded, creating reasonable doubt about evidence tampering.

2. Multiple Handler Issues

Evidence was handled by at least seven different personnel without proper documentation, violating FBI digital evidence handling protocols outlined in the FBI Laboratory Division's Quality Assurance Standards.

C. Attorney-Client Privilege Violations Require Suppression

1. Privileged Communications Accessed

The government's forensic examination accessed over 200 email communications between Mr. Chen and his attorney, Patricia Williams of Williams & Associates, regarding:

- Strategy discussions about this investigation
- Legal advice concerning cybersecurity compliance
- Settlement negotiations in unrelated civil matters

2. Inadequate Screening Procedures

The government failed to implement adequate privilege screening procedures, such as:

- Taint teams to review potentially privileged materials
- Ex ante filtering protocols to identify attorney-client communications
- Court-supervised privilege review procedures

3. Remedy Required

Under *United States v. Ritchie*, attorney-client privilege violations require suppression of all evidence obtained through the privileged communications, including any derivative evidence obtained through investigative leads discovered in those communications.

D. Exceeding Warrant Scope Requires Suppression

1. Temporal Scope Violations

The warrant authorized search for evidence of crimes occurring "between January 2023 and March 2024," yet investigators examined files and communications dating back to 2019, including:

- Business records from Mr. Chen's consulting company
- Personal financial documents unrelated to the alleged crimes
- Communications with other clients regarding legitimate penetration testing

2. Plain View Doctrine Inapplicable

The government cannot rely on the plain view doctrine to justify examination of materials outside the warrant's scope, as established in *United States v. Adjani*, where the Ninth Circuit held that investigators cannot "rummage through" digital files hoping to find evidence of other crimes.

IV. LEGAL AUTHORITIES

Constitutional Authorities

- *Riley v. California*, 573 U.S. 373 (2014)
- *Carpenter v. United States*, 138 S. Ct. 2206 (2018)
- *Groh v. Ramirez*, 540 U.S. 551 (2004)

Circuit Court Precedents

- *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010)
- *United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006)
- *United States v. Burgess*, 576 F.3d 1078 (10th Cir. 2009)

Statutory Authorities

- Federal Rules of Criminal Procedure, Rule 41
- 18 U.S.C. § 1030 (Computer Fraud and Abuse Act)
- Federal Rules of Evidence, Rule 502 (Attorney-Client Privilege)

V. CONCLUSION

The government's search and seizure of Mr. Chen's digital devices violated fundamental Fourth Amendment protections through overbroad warrant language, inadequate privilege protections, and examination beyond the warrant's authorized scope. The integrity of the digital evidence has been compromised through chain of custody violations that create reasonable doubt about authenticity.

These constitutional violations are particularly egregious in cybercrime cases, where the volume of digital evidence requires heightened scrutiny to prevent fishing expeditions through defendants' private digital lives. The remedy for these violations must be suppression of all illegally obtained evidence.

WHEREFORE, Defendant respectfully requests this Court:

1. **GRANT** this Motion to Suppress Digital Evidence;
2. **SUPPRESS** all evidence obtained through the illegal searches described herein;
3. **SUPPRESS** all derivative evidence obtained through leads discovered in the illegally obtained evidence;
4. **DISMISS** all charges that depend upon the suppressed evidence; and
5. **GRANT** such other relief as the Court deems just and proper.

Respectfully submitted,

CYBER DEFENSE LAW GROUP

By: /s/ **Michael Rodriguez**
MICHAEL RODRIGUEZ (SBN 234567)
Attorney for Defendant
555 Montgomery Street, Suite 1200
San Francisco, CA 94111
Telephone: (415) 555-0123
Email: mrodriguez@cyberdefenselaw.com

SARAH K. THOMPSON (SBN 345678)
Of Counsel
Email: sthompson@cyberdefenselaw.com

CERTIFICATE OF SERVICE

I hereby certify that on this 15th day of June, 2024, I served a true and correct copy of the foregoing document upon all parties by electronic filing through the Court's CM/ECF system:

Assistant United States Attorney Jennifer Walsh
Cybercrime Unit
U.S. Attorney's Office
Northern District of California
450 Golden Gate Avenue
San Francisco, CA 94102
Email: jennifer.walsh@usdoj.gov

/s/ **Michael Rodriguez**
MICHAEL RODRIGUEZ

PROPOSED ORDER

Having considered Defendant's Motion to Suppress Digital Evidence, the government's opposition, and oral argument, the Court hereby **ORDERS:**

[ ] Defendant's Motion to Suppress Digital Evidence is **GRANTED**.

[ ] Defendant's Motion to Suppress Digital Evidence is **DENIED**.

[ ] Other: _____

IT IS SO ORDERED.

Date: _____

THE HONORABLE JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

This document is a legal brief template for educational purposes and demonstrates the structure and arguments typically found in cybercrime defense motions.