

**In the Matter of the Recount of Votes  
for President of the United States:**

JILL STEIN,  
c/o Emery Celli Brinckerhoff & Abady LLP  
600 Fifth Avenue, 10<sup>th</sup> Floor  
New York, NY 10020,

Case No.:

Petitioner,

Case Codes: 30701 (Declaratory Judgment)  
30704 (Other Injunction)

v.

WISCONSIN ELECTIONS COMMISSION,  
212 East Washington Avenue  
Third Floor  
Madison, WI 53707, and

Members of the Wisconsin Elections Commission,  
each and only in his or her official capacity:

MARK L. THOMSEN, ANN S. JACOBS,  
BEVERLY GILL, JULIE M. GLANCEY,  
STEVE KING, and DON M. MILLIS  
212 East Washington Avenue  
Third Floor  
Madison, WI 53707,

Respondents.

---

**SUMMONS**

---

THE STATE OF WISCONSIN, To each person named above as a Respondent:

You are hereby notified that the Petitioner named above has filed a lawsuit or other legal action against you. The Complaint, which is attached, states the nature and basis of the legal action.

Within twenty (20) days of receiving this Summons, you must respond with a written answer, as that term is used in Chapter 802 of the Wisconsin Statutes, to the Complaint. The

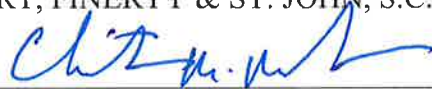
Court may reject or disregard an answer that does not follow the requirements of the statutes. The answer must be sent or delivered to the Court, whose address is Dane County Courthouse 215 South Hamilton Street, Madison, WI 53703-3285, and to Friebert, Finerty & St. John, S.C., Petitioner's attorneys, whose address is 330 East Kilbourn Avenue, Suite 1250, Milwaukee, Wisconsin 53202, ATTN: Christopher M. Meuler, Attorney for Petitioner. You may have an attorney help or represent you.

If you do not provide a proper answer within twenty (20) days, the Court may grant judgment against you for the award of money or other legal action requested in the Complaint, and you may lose your right to object to anything that is or may not be incorrect in the Complaint. A judgment may be enforced as provided by law. A judgment awarding money may become a lien against any real estate you own now or in the future, and may also be enforced by garnishment or seizure of property.

Dated this 28<sup>th</sup> day of November, 2016.

FRIEBERT, FINERTY & ST. JOHN, S.C.

By:



Christopher M. Meuler (SBN: 1037971)

EMERY CELLI BRINCKERHOFF & ABADY,  
LLP

By: Matthew D. Brinckerhoff\*

Debra L. Greenberger\*

David A. Lebowitz\*

*\*Pro hac vice pending*

Attorneys for Petitioner Jill Stein

P.O. ADDRESS:

330 East Kilbourn Avenue, Suite 1250  
Milwaukee, Wisconsin 53202  
Phone: (414) 271-0130

**In the Matter of the Recount of Votes  
for President of the United States:**

JILL STEIN  
c/o Emery Celli Brinckerhoff & Abady LLP  
600 Fifth Avenue, 10<sup>th</sup> Floor  
New York, NY 10020

Petitioner,

Case No.:

v.

WISCONSIN ELECTIONS COMMISSION  
212 East Washington Avenue  
Third Floor  
Madison, WI 53707, and

Case Codes: 30701 (Declaratory Judgment)  
30704 (Other Injunction)

Members of the Wisconsin Elections Commission,  
each and only in his or her official capacity:

MARK L. THOMSEN, ANN S. JACOBS,  
BEVERLY GILL, JULIE M. GLANCEY,  
STEVE KING, and DON M. MILLIS  
212 East Washington Avenue  
Third Floor  
Madison, WI 53707,

Respondents.

---

**COMPLAINT AND PETITION  
FOR AN ORDER PURSUANT TO WISCONSIN STATUTES §§ 5.90(2) AND 9.01**

---

Jill Stein, by her undersigned attorneys, hereby files this complaint and petition and alleges as follows:

**INTRODUCTION**

Petitioner Jill Stein was a candidate for the office of the President of the United States in an election held on November 8, 2016. On November 25, 2016, Petitioner filed with Respondent

the Wisconsin Elections Commission a verified petition for a recount of all ballots in all wards in the State of Wisconsin pursuant to Wisconsin Statutes § 9.01. Ms. Stein’s verified petition requested a hand recount of all ballots, but applicable law affords discretion to the various boards of canvassers throughout the State to recount most ballots cast throughout Wisconsin either by hand or with “automatic tabulating equipment.” *See* Wis. Stat. § 5.90(1). However, this court has the power to order a hand recount. Wis. Stat. § 5.90(3). The prospect of a recount performed with “automatic tabulating equipment”—the same equipment Ms. Stein’s recount petition explained may have been attacked by foreign government agents seeking to interfere in the presidential race—risks tainting the recount process. Petitioner seeks an order for a hand recount of all optical scan ballots, *i.e.* ballots “distributed to the electors.” Wis. Stat. § 5.90(1).

### **PARTIES**

1. Plaintiff Jill Stein was the Green Party nominee for President of the United States in the 2016 election.

2. Respondent Wisconsin Elections Commission (“Elections Commission”) is an agency of the State of Wisconsin, which is endowed by statute with the responsibility for the administration of all laws relating to elections and election campaigns. *See* Wis. Stat. § 5.05.

3. Respondents Mark L. Thomsen, Ann S. Jacobs, Beverly Gill, Julie M. Glancey, Steve King, and Don M. Millis, each personally and individually but only in his or her official capacity, are all members of the Wisconsin Elections Commission.

### **JURISDICTION AND VENUE**

4. This Court has jurisdiction over this matter pursuant to Wis. Stat. § 5.90(2)-(3).

5. Venue is proper in this judicial district pursuant to Wis. Stat. § 801.50(5t).

## FACTUAL ALLEGATIONS

### Background

6. On November 25, 2016, Petitioner filed with the Elections Commission a sworn petition for a recount of votes cast in the State of Wisconsin for President of the United States in the 2016 election.

7. The logistics of the recount process depend upon the type of voting equipment used in a particular locality. Of particular relevance here are the two primary electronic voting systems used in Wisconsin: “optical scan” and “direct-recording electronic” (“DRE”) voting. An optical scan system uses an electronic scanner to read paper ballots that have been marked by the voters directly and to tabulate the results. DRE machines allow voters to indicate their vote using touchscreens, after which a computer processes their vote records the result in a removable memory component. DRE machines produce a “voter-verified paper audit trail” (“VVPAT”) at the time each vote is cast. The VVPAT is a paper record of each vote cast, that is printed out to be inspected and available to be verified by the voter immediately upon casting his or her vote. By contrast, in optical scan voting, a ballot is distributed to each voter, who completes it him- or herself.

8. Under Wisconsin law, where DRE machines are used, “the board of canvassers shall perform the recount using the permanent paper record of the votes cast by each elector, as generated by the machines.” Wis. Stat. § 5.90(1). However, “if the ballots are distributed to the electors,” as is the case where optical scan voting is used, boards of canvassers have the option of performing the recount “with automatic tabulating equipment,” entirely “by hand,” or “by hand for only certain wards or election districts.” *Id.*

9. Candidates may seek a court order requiring that a recount be done by hand.

Pursuant to Wis. Stat. § 5.90(2):

Any candidate, or any elector when for a referendum, may, by the close of business on the next business day after the last day for filing a petition for a recount under s. 9.01, petition the circuit court for an order requiring ballots under sub. (1) to be counted by hand or by another method approved by the court. The petitioner in such an action bears the burden of establishing by clear and convincing evidence that due to an irregularity, defect, or mistake committed during the voting or canvassing process the results of a recount using automatic tabulating equipment will produce incorrect recount results and that there is a substantial probability that recounting the ballots by hand or another method will produce a more correct result and change the outcome of the election.

10. Here, where the overall integrity of the election cannot be verified by an automatic recount and popular acceptance of the winner is severely impaired, a hand recount is warranted. The Wisconsin Supreme Court has recognized that courts may relax the standard of outcome-determinativeness generally applied to election irregularities where such irregularities are “so significant in number or so egregious in character as to seriously undermine the appearance of fairness, . . . even when the outcome of the election might not be changed.” *McNally v. Tollander*, 100 Wis. 2d 490, 504, 302 N.W.2d 440 (1981). In post-election proceedings the “primary concern” must be “the protection of the rights and interests of the voters.” *Roth v. Lafarge Sch. Dist. Bd. of Canvassers*, 2004 WI 6, 268 Wis. 2d 335, 349, 677 N.W.2d 599. *See also* Wis. Stat. § 5.01(1) (providing that election laws “shall be construed to give effect to the will of the electors”).

**The Unique Circumstances of the 2016 Presidential Election Require a Hand Recount**

11. The 2016 presidential election was subject to unprecedented cyberattacks apparently intended to interfere with the election. This summer, attackers broke into the email system of the Democratic National Committee and, separately, into the email account of John

Podesta, the chairman of Democratic Party candidate Hillary Clinton's campaign. The attackers leaked private messages from both hacks. Attackers also infiltrated the voter registration systems of two states, Illinois and Arizona, and stole voter data. The Department of Homeland Security has stated that senior foreign government officials commissioned these attacks. Attackers attempted to breach election offices in more than 20 other states. *See* Affidavit of J. Alex Halderman ("Halderman Aff."), ¶ 7 & Exs. A, B, C, D, E, F.

12. If a foreign government were to attempt to hack American voting machines to influence the outcome of a presidential election, one might expect the attackers to proceed as follows. First, the attackers might probe election offices well in advance to find ways to break into the computers. Next, closer to the election, when it was clear from polling data which states would have close electoral margins, the attackers might spread malware into voting machines into some of these states, manipulating the machines to shift a few percent of the vote to favor their desired candidate. One would expect a skilled attacker's work to leave no visible signs, other than a surprising electoral outcome in which results in several close states differed from pre-election polling. *See* Halderman Aff., ¶ 9.

13. Experts have repeatedly documented in peer-reviewed and state-sponsored research that American voting machines have serious cybersecurity problems. Voting machines are computers with reprogrammable software. An attacker who can modify that software by infecting the machines with malware can cause the machines to provide any result of the attacker's choosing. In just a few seconds, anyone can install vote-stealing malware on a voting machine that silently alters the electronic records of every vote. *See* Halderman Aff., ¶ 10. Practically speaking, it is not possible to determine with certainty the absence of malicious

software hiding within what might appear to be many thousands of lines of legitimate software code. *See* Affidavit of Poorvi L. Vora (“Vora Aff.”), ¶ 13.

14. Whether voting machines are connected to the Internet is irrelevant. Sophisticated attackers such as nation-states have developed a variety of techniques for attacking non-Internet-connected systems. Shortly before each election, poll workers copy the ballot design from a regular desktop computer in a government office (or at a company that services the voting machines) and use removable media (akin to the memory card in a digital camera) to load the ballot design onto each machine. That initial computer is almost certainly not well enough secured to guard against attacks by foreign governments. If technically sophisticated attackers infect that computer, they can spread vote-stealing malware to every voting machine in the area. Most voting machines also have reprogrammable software (“firmware”) that can in many cases be manipulated well in advance of the election to introduce vote-sealing malware. Technically sophisticated attackers can accomplish this with ease. Halderman Aff., ¶ 11; *see also* Affidavit of Dan S. Wallach (“Wallach Aff.”), ¶ 7 (“Combine the patience and resourcefulness of a nation-state adversary with the unacceptably poor state of security engineering in our voting systems,” and it becomes “entirely reasonable to consider attacks against our voting systems to be within the feasible scope of our adversaries’ capabilities”); Affidavit of Ronald L. Rivest (“Rivest Aff.”), ¶ 8 (“We have learned the hard way that almost any computer system can be broken into by a sufficiently determined, skillful, and persistent adversary. There is nothing special about voting systems that magically provides protection against attack.”); Affidavit of Harri Hursti (“Hursti Aff.”), ¶¶ 6-22 (detailing various attack vectors to which optical scan voting systems are vulnerable). AV-OS tabulators—which are among the optical scanners used in Wisconsin—have been proven to be vulnerable to serious



security threats and hacks capable of neutralizing or swapping candidates or reporting results incorrectly. *See* Vora Aff., ¶ 25 (noting that “one can carry out a devastating array of attacks against an election using only off-the-shelf equipment and without having ever to access the card physically or opening the AV-OS system enclosure”).

15. While the vulnerabilities of American voting machines have been known for some time, states’ responses to these vulnerabilities have been patchy and inconsistent at best. Many states, including Wisconsin, continue to use out-of-date machines that are known to be insecure. Halderman Aff., ¶ 12.

16. Procedural safeguards used by Wisconsin and other states to protect their voting equipment are inadequate to guard against manipulation of the election outcome via cyberattack. These inadequate safeguards include tamper evident seals, protective counters, and test decks. Tamper evident seals do not protect against remote electronic attackers, and may not even defend against local attackers. Malware installed on a voting machine can subvert the protective counter by changing its value in the machine’s computer memory. Malware can subvert test decks by refraining from cheating when only a small number of ballots have been scanned (as is the case when a test deck is used), or by only cheating at a specified time of day (electronic voting machines typically have internal clocks). Halderman Aff., ¶ 13.

17. The companies that provide and service election equipment for municipalities are another possible target for attackers. An example of such as a vendor is Command Central Elections, a small business in Minnesota that provides voting machines to approximately 1000 municipalities in Wisconsin. In many municipalities, Command Central is responsible for updating voting machine software and programming ballot designs prior to the election. Such companies provide an attractive target for attackers, since compromising their computer systems

would allow an attack to spread to voting machines over much of the state. An attack on Command Central could affect election in hundreds of jurisdictions statewide by altering the software or election media in malicious ways that could go detected absent a manual examination of the ballots. Halderman Aff., ¶ 14.

18. A study published by Professor Walter R. Mebane of the University of Michigan finds statistical abnormalities in ward-level vote data from Wisconsin that are consistent with fraud having taken place in the 2016 presidential election. Wards are the smallest aggregation unit at which vote counts are reported in Wisconsin. Mebane, a statistician and political science professor, used election forensics techniques designed to identify electoral fraud. He discovered an “array of anomalies” in the small wards with optical-scan technology which do not occur in the small wards without optical-scan technology. He also discovered some anomalies in specific optical-scan machines in big wards. Mebane concludes that the data published by Wisconsin so far makes it difficult to establish whether or not reported vote counts accurately reflect the intentions of the electors, but that “[a] rigorous audit or a full recount that has humans manually checking the paper ballots can provide convincing evidence about who won the election.” See Affidavit of Philip B. Stark (“Stark Aff.”), ¶ 38 (describing how Mebane’s analysis “raises suspicion about the accuracy of counts in some wards that voted using optical scan voting systems”).

19. Paper ballots are the best and most secure technology available for casting votes. Optical scan voting allows the voter to fill out a paper ballot that is scanned and counted by a computer. Electronic voting machines with voter-verified paper audit trails allow the voter to review a printed record of the vote he has just cast on a computer. Only a paper record

documents the vote in a manner that cannot later be modified by malware or other forms of cyberattacks. Halderman Aff., ¶ 15.

20. The only way to determine whether a cyberattack affected the outcome of the 2016 presidential election is to examine the available physical evidence—that is, to count the paper ballots and paper audit trail records, and review the voting equipment, to ensure that the votes cast by actual voters match the results determined by the computers. Halderman Aff., ¶ 17. While Wisconsin law requires reviewing the paper audit trail records from DRE machines, this Petition is necessary to require all counties to count the paper ballots that were initially tabulated by optical scanners.

21. For ballots cast through optical scanners, a manual recount of the paper ballots, without relying on the electronic equipment, is necessary to reliably detect possible hacking. Using optical scan machines to conduct the recount, even after first evaluating the machines through a test deck, is insufficient to detect potential cyberattacks. Attackers intending to commit a successful cyberattack could, and likely would, create a method to undermine any pre-tests. Halderman Aff., ¶ 19.

22. If the scanners were attacked by infecting them with malware, such malware might still be active in the machines during the recount. Recounting the ballots using an infected scanner would likely yield the same results as the original count, despite the results being wrong. Halderman Aff., ¶ 20; *see also* Wallach Aff., ¶ 14 (“A purely electronic tally of paper ballots, without some sort of hand-counting or auditing would be unable to detect systematic electronic tampering—the very risk we’re concerned about in this election.”); Stark Aff., ¶ 24 (“Rescanning and retabulating without checking the electronic data against the original paper records cannot confirm that the reported result is correct.”); Hursti Aff., ¶ 4 (“Optical scan machines can be

hacked in a manner that changes election results, and such an attack would likely go undetected during normal pre- and post-election testing. If the scanners are hacked, using them as part of the recount process is likely to result in the same fraudulent election outcome.”).

23. If attackers managed to compromise the count during election day but in a manner that did not persist on the machines, machine recounts would still be insufficient. Attackers who were able to infect the machines before the election likely would be able to attack them again, perhaps using the same methods, prior to the recount. This would result in the scanners producing the same incorrect results when the ballots were scanned again. Halderman Aff., ¶ 21.

24. In contrast to machine recounts, a manual recount, where the paper ballots are inspected by humans, can reliably detect any cyberattack that might have altered the election outcome on the optical scanners. Halderman Aff., ¶ 22.

25. To accurately verify the outcome of soft-ware based voting systems requires a software-independent system, *i.e.*, a system that has a means of verifying the election outcome independent of the software that computed it. *See* Vora Aff., ¶ 14. Securely-stored paper records must be examined to ensure that they are consistent with the election outcomes declared by the voting system software. If they are not examined, any unintentional software bugs, intentional alterations to the vote or to the tally, or procedural errors leading to an incorrect election outcome will not be detected. *Id.*, ¶ 17.

26. A manual recount is the best way, and indeed the only way, to ensure public confidence that the results are accurate, authentic, and untainted by interference. It will also set a precedent that may provide an important deterrent against cyberattacks on future elections. Halderman Aff., ¶ 22; *see also* Wallach Aff. ¶ 7 (“The mere *possibility* of a recount or audit of the paper ballots acts as a deterrent to an electronic attack; it’s much more difficult to tamper

with paper, in bulk, relative to the effort to tamper with purely electronic records as used in many states (but not Wisconsin).”); Rivest Aff. ¶ 36 (“It is important to emphasize that an audit or a recount really *must* look at the paper ballots. Otherwise one is not examining the primary election data (the cast ballots themselves) but only derivative secondary data that may have been corrupted by faulty or malicious software.”)).

27. Indeed, according to a recent Washington Post-ABC News Poll, 18% of Americans surveyed—and 33% of supporters of Democratic Party candidate Hillary Clinton—do not accept Republican candidate Donald Trump’s election as legitimate. Scott Clement, *One-third of Clinton supporters say Trump election is not legitimate, poll finds*, WashingtonPost.com (Nov. 13, 2016).<sup>1</sup> A hand recount is needed to shore up public confidence in the outcome of the election. See Rivest Aff. ¶ 20 (“For our democracy to work well, election systems should produce the best and most convincing evidence that announced election outcomes are correct. One should ask: what will it take to convince a skeptical supporter of a losing candidate that they really lost? Evidence of the form, ‘You must trust the computer here.’ is not likely to be adequate (nor should it be).”).

**A Hand Recount Is Feasible and No More Burdensome than Electronic Retabulation**

28. It is important to note that hand recounts—even for statewide races—are common and practicable.

29. For example, in 2011, Wisconsin conducted a statewide recount of votes cast in the Wisconsin Supreme Court election. According to the Elections Commission, in the initial counting of votes after the election, “90 percent of the ballots were cast on paper and counted by optical scanners, 5 percent were cast on paper and counted by hand, and 5 percent were cast and

---

<sup>1</sup> Available at <https://www.washingtonpost.com/news/the-fix/wp/2016/11/13/one-third-of-clinton-supporters-say-trump-election-is-not-legitimate-poll-finds/>.

tabulated on touch-screen equipment.” See <http://elections.wi.gov/elections-voting/recount/ballot-authenticity>. However, in the recount, “of the 90 percent that were originally counted by voting equipment on Election Night, more than half” were “recounted by hand.” *Id.* As the Elections Commission acknowledged then, hand recounting resulted “in some ballots being counted that the voting equipment may not have attributed a vote due to ballot irregularity, such as the voter circling the candidate name instead of filling in the oval or arrow.” This finding is consistent with expert research on optical scanning, which consistently finds that optical scanners misinterpret votes for various reasons. See, e.g., *Vora Aff.*, ¶ 22; *Wallach Aff.*, ¶¶ 17-21; *Stark Aff.*, ¶¶ 27-32; see generally Affidavit of Douglas W. Jones. Hand counting is therefore also most consonant with Wisconsin’s policy of giving effect to the intent of the voter. See *Roth*, 268 Wis.2d at 329 (“ballots are the best evidence of the intention of voters”).

30. The Elections Commission has itself acknowledged that a hand recount is not necessarily more time-consuming than an electronic retabulation. In a November 25, 2016 message to all of the County Clerks in Wisconsin, Elections Supervisor Ross Hein stated: “In discussions with Wisconsin election officials over the years, a hand-count may not be as timing [sic] consuming as one may think and avoids pre-testing of the equipment and reprogramming of memory devices.” See <http://elections.wi.gov/node/4439>.

31. This statement is consistent with practical experience in other jurisdictions such as Minnesota, where, according to published sources, a hand recount of all of the more than two million votes cast in the 2010 statewide race for Governor was completed in approximately five days.

32. In short, manual recounts are not necessarily more time-consuming than recounting using optical scanners. A manual recount focuses on a single contest, and human

observers typically proceed by sorting the ballots into stacks according to the chosen candidate and then counting the ballots in each stack. This is an efficient and straightforward process. If scanners are used, the scanners must be programmed and tested, and the ballots must be fed into the scanner by humans. These steps are not necessary when hand counting is used. Halderman Aff., ¶ 23.

33. The paper ballots used in Wisconsin can be counted much more easily and reliably than the punched card paper ballots that were recounted in Florida during the 2000 presidential election. Punched card ballots are fragile, so each time they are counted, the record of voters' intent may be inadvertently altered. They are also difficult to interpret, sometimes requiring a magnifying glass to discern whether the voter intended to make a mark. Wisconsin's optically scanned paper ballots are a completely different technology. They create a persistent and readily interpretable record of voters' intent that does not suffer from these problems, and they can be counted efficiently and accurately in a manual recount. *Id.*, ¶ 24.

34. Any contemplated efficiency benefit to an electronic retabulation is especially illusory because, in any locality that proceeds to use optical scanning machines to perform a recount, Petitioner plans to exercise her right to inspect each ballot before it is inserted into the tabulator. *See* Wisconsin Elections Commission, *Election Recount Procedures*<sup>2</sup> at 12 (Nov. 2016) ("Each ballot . . . may be inspected by the candidates or their representatives before being inserted into the tabulator."); Wis. Stat. § 9.01(b)(11) ("All steps of the recount shall be performed publicly . . . . [A]ll materials and ballots may be viewed and identified by the candidates . . . ."). Accordingly, an electronic retabulation will be no faster or more efficient than a hand recount.

---

<sup>2</sup> Available at [http://elections.wi.gov/sites/default/files/publication/65/recount\\_manual\\_11\\_2016\\_pdf\\_17034.pdf](http://elections.wi.gov/sites/default/files/publication/65/recount_manual_11_2016_pdf_17034.pdf).

35. Furthermore, Petitioner has paid or will pay all fees associated with the statewide recount. *See* Wis. Stat. § 9.01(1)(ag)(3). The public fisc will therefore be unaffected by any order to conduct a hand recount.

**COUNT 1**

**PETITION**

**FOR AN ORDER PURSUANT TO WISCONSIN STATUTES §§ 5.90(2) AND 9.01**

36. Petitioner repeats and realleges the foregoing paragraphs as if set forth fully herein.

37. Due to an irregularity, defect, or mistake committed during the voting or canvassing process, the results of any recount using automatic tabulating equipment will produce incorrect recount results.

38. There is a substantial probability that recounting the ballots by hand will produce a more correct result and change the outcome of the election.

**WHEREFORE**, Petitioner respectfully requests judgment as follows:

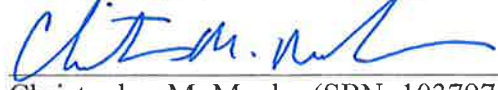
- A. An order to recount all ballots in all wards in the State of Wisconsin by hand.
- B. Such other and further relief as the court may deem just and equitable.



Dated this 28<sup>th</sup> day of November, 2016.

FRIEBERT, FINERTY & ST. JOHN, S.C.

By:



Christopher M. Meuler (SBN: 1037971)

EMERY CELLI BRINCKERHOFF & ABADY,  
LLP

By: Matthew D. Brinckerhoff\*  
Debra L. Greenberger\*  
David A. Lebowitz\*

*\*Pro hac vice admission pending*

Attorneys for Petitioner Jill Stein

P.O. ADDRESS:

330 East Kilbourn Avenue, Suite 1250  
Milwaukee, Wisconsin 53202  
Phone: (414) 271-0130