

My name is Michael. I'm an Oakland resident and a software engineer with 40 years' experience. I've been taking an interest in the success of the Democracy Dollars project for a couple years now.

On this month's ED's report of Q3 major projects, I noticed that the bullet point "Determine technical requirements for Democracy Dollars ID-verification and signature verification process" that was present in the May report has been removed. I'm concerned about delaying this, since I see it as an important issue in addressing the ease of use of the online system and the associated financial savings.

costs

It has been raised in PEC public comments that the cost of administering Seattle's democracy vouchers program was \$1.4M for \$700k in candidate distributions. While this number is correct for the 2024 election year, for the whole six-year period 2020-2025 the total administrative costs were about 70% of the total candidate distributions.ⁱ This still seems high to me, though we don't have other examples against which to compare it.

Given the fiscal state of the city and the PEC's current dependence on the city council for funding—or likewise, given any intent that the PEC may have for obtaining direct funding from a tax measure—it seems prudent to reduce these costs as much as possible. The Seattle program's report says that only 27% of the donors used the online system in 2025.ⁱⁱ This seems like an area ripe for cost-reduction by encouraging use of the online system and/or discouraging the paper-based and in-person systems.

data security

For-profit companies have repeatedly breached the trust given to them. In the appendix I list some recent data breaches that affect the sort of data that we seem to be proposing to collect, if we follow in the pattern of Seattle.

That's not to impugn Seattle's vendor, Trulioo—they so far appear to have a good track record at protecting dataⁱⁱⁱ—and I expect that the PEC would take similar care in choosing a reputable (and not necessarily cheap) vendor.^{iv} Instead my concern is about the impression that these breaches have left on the public consciousness, leading them to distrust for-profit companies.

My suspicion, which would need to be confirmed with Seattle, is that the 27% use of their online system is due to this distrust. And since the cost is tied to the use of non-electronic media, such distrust would have a direct impact on Oakland's costs.

Keeping the residents' PII in the hands of the county or state may improve the use of online processes. Governments tend to provide better protection of PII, because they're not motivated by profit and competing on the lowest price. The City of Oakland itself, however, notably had a breach in 2023. Protection is likely better at the county or state level, where they have more resources.

Providing safe handling of PII is also an equity issue: Poorer residents are least able to defend themselves against a data breach, due to the resources needed. They're also the most vulnerable to losses from a breach. So they're likely to avoid the online process if they feel it might expose them to breaches.

So the ideal, then, if this logic holds, is that the Democracy Dollars system should verify its users purely through government-controlled systems. The government is, after all, the arbiter of who is an eligible resident and should have all the data to verify that.

While there may be subsequent authentication concerns, authentication to the standards of the county for voting purposes provides the baseline of what we'd need to accomplish. Since Democracy Dollars involves the transfer of \$1M in \$100 increments, it may require more extensive authentication than what we're willing to accept in California for the right to vote. But I envisage that to be done by augmenting voting authentication, in other words, by taking advantage of the system already in place.

questions

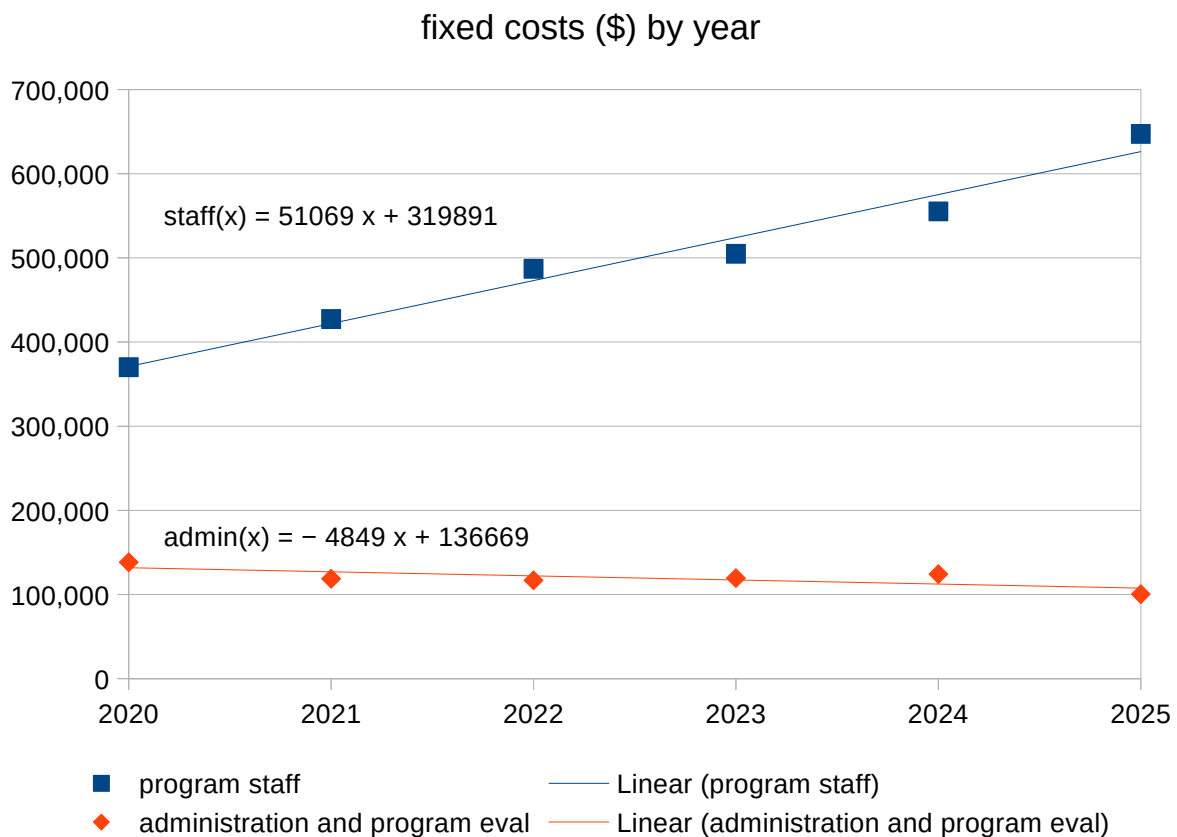
1. I'd like to understand why this goal was removed from the stated Q3 goals.
2. If PEC staff aren't going to pursue this question, I'd like the PEC to support volunteers—like myself and those in OpenOakland—to pursue it directly with the county and/or state and collect whatever information that we can.
3. The PEC seems to be going ahead with development of the Democracy Dollars software. The authentication of donors is going to be one of the first problems that will need to be addressed. What plan does the PEC have for this? Are they going to simply follow the approach that Seattle uses?
4. Can we get clarity on what Seattle is doing, or has tried, to reduce its costs?

appendix

Seattle's costs

Oakland has a population that's roughly 45% smaller than Seattle's, so all the numbers here should be reduced proportionately for comparison.

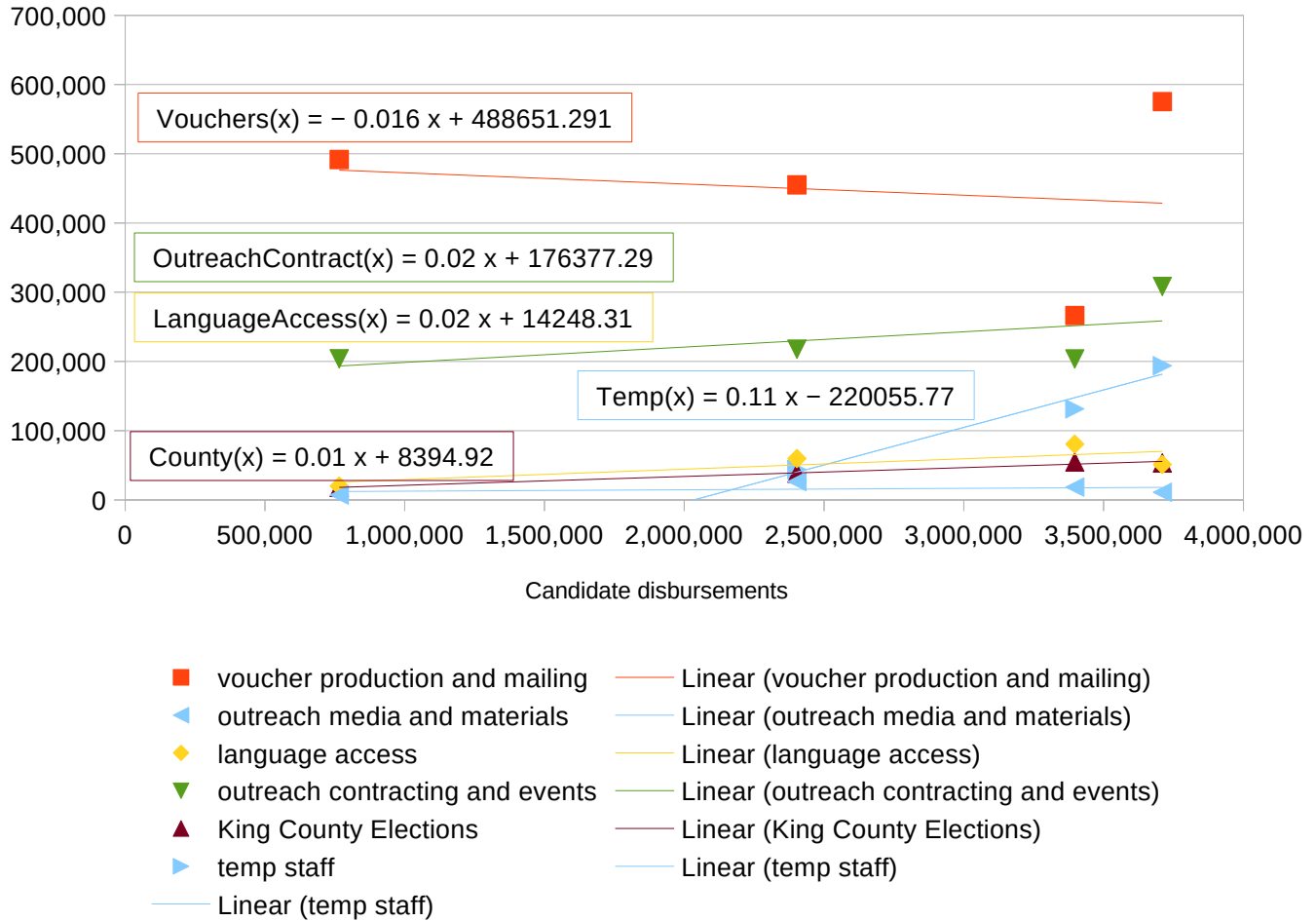
The expenses for the Seattle voucher program can be broken down into fixed costs and “variable” costs. The fixed costs include the staff salaries and the cost of administration and evaluation:



Administrative costs are fairly stable around \$120k/year, while staff costs are around \$650k/year, rising \$50k/year.

The “variable” costs are then those that only occur during election years, which is normally every other year, but also includes special elections. These costs don't actually vary much across the election years.

election costs (\$) vs. disbursements (\$)



The main anomaly in the pattern is that voucher production and mailing per candidate disbursement cost significantly less in 2021. Otherwise, costs are roughly fixed, with a slight (1-2%) positive correlation with disbursements. Temporary staff costs naturally kick in when the number of vouchers to process exceeds a level that staff can handle.

data breaches

This is a list of data breaches that I've been collecting just since late 2024 that relate to the sort of data collection that we're proposing in this system. All of them are by for-profit entities, not government, but exclude intentional acts such as those allegedly committed under DOGE.

1. In December 2024, an Indian startup that provides KYC services for financial institutions globally “exposed customer IDs, addresses, contact numbers, and video recordings”.^v
2. Prior to December 2024, a U.S. online gift card store “was publicly exposing hundreds of thousands of customer government-issued identity documents to the internet”^{vi}
3. An Oakland business owner, serving as an AML compliance officer, “kept 15,000 images of identity cards from California, Honduras and Mexico” as part of his money laundering scheme.^{vii}
4. In October 2025, the chat application Discord exposed 70,000 users’ government ID photos or related sensitive data via a third-party provider, as part of their age verification process.^{viii}
5. In January 2025, Conduent, a company that provides government and corporate benefits services “compromised individuals’ names, dates of birth, addresses, Social Security numbers, health insurance information, and medical data” for over 25 million people across the U.S.^{ix}
6. Prior to May 2026, a prison calling service over 300,000 scanned driver’s licenses. In June 2025, the same company was the subject of a ransomware attack that exfiltrated data including over 10,000 video calls and 10,000 audio calls by inmates.^x
7. In June 2026, a breach of a vendor to the Texas Parks & Wildlife department “allowed hackers to take the driver’s license information and passport numbers of more than 3 million people”.^{xi}

- i “Democracy Voucher Program 2025 Annual Report”,
<https://www.seattle.gov/documents/Departments/EthicsElections/DemocracyVoucher/Biennial%20Reports/2025%20Democracy%20Voucher%20Program%20Report%20Final.pdf>, p. 10
- ii Ibid., p. 6
- iii <https://www.upguard.com/security-report/trulioo>
- iv Trulioo had been charging Seattle \$10k/year but was raising the price to \$20k.
- v <https://economictimes.indiatimes.com/tech/technology/financial-institutions-double-down-on-more-checks-for-tech-partners/articleshow/116115049.cms>
- vi <https://techcrunch.com/2025/01/03/online-gift-card-store-exposed-hundreds-of-thousands-of-peoples-identity-documents/>
- vii <https://www.sfchronicle.com/crime/article/oakland-business-owner-sentenced-prison-money-20041436.php>
- viii <https://techcrunch.com/2025/10/09/discord-suffers-data-breach-impacting-at-least-70000-users/>
- ix <https://techcrunch.com/2026/02/24/conduent-data-breach-grows-affecting-at-least-25m-people/>
- x <https://techcrunch.com/2026/05/28/a-security-lapse-at-prison-payphone-service-pay-tel-publicly-exposed-over-300000-callers-drivers-licenses/>
- xi <https://techcrunch.com/2026/06/18/texas-government-data-breach-allowed-hackers-to-steal-3-million-drivers-licenses-and-passports/>