



STATE OF CALIFORNIA
FAIR POLITICAL PRACTICES COMMISSION
1102 Q Street • Suite 3050 • Sacramento, CA 95811
(916) 322-5660 • Fax (916) 322-0886

To: Chair Silver, Commissioners Brandt, Ortiz, and Wilson

From: Dave Bainbridge General Counsel, Legal Division
Zachary W. Norton, Senior Counsel, Legal Division

Subject: Prenotice Discussion, Proposed Amendments to Regulations 18401, 18421.3, and 18430.1.

Date: June 9, 2025

Executive Summary

Staff proposes:

- Additional detailed verification and recordkeeping requirements for monetary contributions collected by contract vendors or collection agents on behalf of candidates and committees.
- Prohibiting a candidate or committee from purchasing or using a prepaid debit, prepaid credit, or gift card in an amount of \$100 or more.
- Prohibiting a candidate or committee from accepting any contributions totaling \$100 or more of, or made using, a prepaid debit, prepaid credit, or gift card, which is consistent with the rules regarding the acceptance of cash contributions.

Staff presents these proposed amended regulations for pre-notice discussion, with adoption proposed for the August 2025 Commission meeting.

Reason for Proposed Regulatory Action

These proposed amendments arose from work done by the Enforcement Division, where Special Investigators identified several cases of misuse and nondisclosure involving third-party payment processors (“TPPs”) that provided services to candidates and committees relating to either contribution solicitations or expenditure payments. These proposed amendments would require more accurate verification and detailed recordkeeping to ensure accurate identification and disclosure of contributors who use online contribution platforms. The proposal will also restrict expenditures for prepaid cards, including gift cards, to less than \$100, as well as prohibit contributions of, or made with, prepaid cards and gift cards in amounts of \$100 or more.

Background

The Political Reform Act was created to accomplish several purposes, one such purpose being that the receipts and expenditures in election campaigns be fully and truthfully disclosed in order that the voters may be fully informed and improper practices may be inhibited. (Section 81002.) In furtherance of this goal, the Act requires committees to file periodic campaign statements disclosing contributions and expenditures. (Sections 84200 - 84225.) Section 84211 specifies what information must be disclosed on campaign statements and requires specific disclosure concerning the identity of contributors.

The Act contains disclosure and recordkeeping requirements with respect to contributions and expenditures, and prescribes the manner in which contributions and expenditures of \$100 or more may be made. (Section 84200 et seq.; and Section 84300(c).) Specifically, no contribution of \$100 or more may be made or received in cash, and a contribution of \$100 or more must be in the form of a written instrument containing the name of the contributor and drawn from the account of the contributor. Similarly, no expenditure of campaign funds of \$100 or more may be made in cash. (Section 84300 (a), (b) & (c).) For each contributor of \$100 or more, a committee must disclose the contributor's full name, street address, and, if the contributor is an individual, the contributor's occupation and employer. (Section 84211(f).)

Internet Fundraising

The Act also permits candidates and committees to raise contributions over the Internet, as long as the Act's disclosure and recordkeeping requirements are met. Regulation 18421.3, meanwhile, details the reporting requirements for contributions and expenditures collected by "contract vendors" or "collection agents."

These contract vendors or collection agents provide platforms for collecting contributions electronically, typically through a web page, on behalf of the candidates or committees. These vendors use TPP to process the contributions, which are then held in temporary accounts before transfer to the candidates' or committees' campaign bank accounts. In addition, these vendors also collect contributor information, provided to the vendors by the individual contributors when the electronic contributions are made. This information is then provided to the committees along with the corresponding contributions.

Third-Party Payment Processors

Third-party payment processors, or TPPs, are financial institution customers that provide payment processing services to merchants and other entities, typically initiating transactions on behalf of merchant clients that do not have a direct relationship with the payment processor's financial institution. TPPs use their own deposit accounts at a financial institution to process such transactions and sometimes establish deposit accounts at the financial institution in the names of their merchant clients.

As with many online purchases, payment information is often encrypted for consumer and data protection. This is problematic from a campaign reporting compliance and enforcement

perspective when a contribution platform is unable to access payee information due to data encryption and its own internal data collection processes. Thus, the contribution platform itself is unable to review cardholder information and cross-reference it with the disclosure provided by the contributor to verify the information.

Enforcement Division staff recently identified several instances of this activity. In one case, a TPP was asked to provide cardholder information, and the same card number had been identified as being used for multiple campaign contributions online. Due to its data encryption policies, the TPP was unable to provide any additional information beyond what the contributor had provided. Enforcement Special Investigators found that the contributor was responsible for entering both cardholder *and* contributor information, with no requirement that the cardholder's name and the contributor's name match for the transactions to be authorized. The contributor was allowed to enter the same card information multiple times with different contributor information. In this case, the committee did not notice that the same card was used as a payment method for different contributors.

Enforcement Division Special Investigators have also revealed that some TPPs provide equipment used to facilitate in-person payments. These are point-of-sale ("POS") systems that provide hardware and software typically used by small businesses to process payments. Essentially, they are small, portable electronic devices, similar in size to a smartphone, that would allow a contributor to swipe or tap a card to make a contribution. These POS systems can code payments as cash, leaving the recipient responsible for keying in the correct payment type. Although these POS devices make it easier for committees to accept contributions, the use of these devices can make it difficult to verify contributor information and the payment source. They also allow for the acceptance of cash, as seen in a recent Enforcement investigation.

Address Verification Service

"Address Verification Service" ("AVS") is a verification and security feature where the billing address entered by the payer is compared with the records held by the card issuer at the time of a transaction to confirm they match. AVS occurs during the card authorization portion of a transaction. Upon accepting payment information, the business's payment processor reaches out to the bank that issued the card with a request to authorize the purchase. During authorization, the issuer checks to ensure that adequate funds or credit exist to cover the transaction, the card is valid, the card verification value ("CVV") code (the three- or four-digit code located on the back of the card next to the signature line) matches the number provided during the transaction, and that the billing address provided during checkout matches the address on file for the card.

However, there are limitations to the level of verification provided by AVS. The primary purpose of AVS is to limit fraud by ensuring that the card is valid, with available funds, and that its use is authorized by the cardholder. As the name suggests, AVS verifies the address, not the name, on the card. Contract vendors that use TPPs to collect contributions have confirmed that they cannot obtain the name on the card from the processor. AVS verifies the numeric portions of the billing address and does not confirm the cardholder's name. This means that while AVS can help detect address discrepancies, it does not ensure that the name on the payment method matches the contributor's name. While the Act requires disclosure of a contributor's street

address, the cards themselves may be tied to a business address or PO Box. AVS is set up to check the billing address and zip code provided by the cardholder with the billing information on file with the card issuer. While this is designed to protect against the use of stolen cards (where the person in possession of a stolen card would not likely know this information), it does not ensure verification of the identity of the person making the contribution with the card.

In addition, contract vendors use other means to help verify transactions. This includes technology to determine the Internet Protocol address (“IP address”) of contributors using their platforms. This provides additional information to ensure that only valid contributions are accepted. A payment originating from a foreign IP would be flagged for internal review as a possible prohibited foreign contribution, while multiple contributions made from the same billing address, IP address, and credit card would also be flagged for further review by the processor. Inquiry by the payment processor would then determine whether these contributions should be accepted, such as in instances where a contributor is traveling overseas at the time a contribution is made, accounting for the foreign IP address, or where spouses who share a credit card each make contributions this the card, account for the duplicate information.

Prepaid cards

Prepaid access is defined as “access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number, or personal identification number.”¹ This includes gift cards, which may or may not be tied to specific retailers, and prepaid cards, including prepaid debit and prepaid credit cards. Prepaid cards, and particularly gift cards, may take the form of a physical card, or a virtual card, where the card number and pin are sent directly to the recipient’s email address. Banks can offer access to prepaid debit and credit cards to a wider range of customers because there is less credit or nonpayment risk than with other means of payment. Prepaid access devices also provide customers easy, anonymous access to funds when transactions are conducted through electronic channels such as the Internet.² A prepaid debit or credit card is much like a gift card, as it allows users to spend whatever amount of money is stored on the card. The card can be reloaded online or at an ATM, a participating store, or another physical location when the balance is used up. Prepaid debit and credit cards are issued by banks and are branded by the major credit card companies, including Visa, MasterCard, Discover, and American Express. They are readily available and may be purchased online and from a variety of physical locations, such as local bank branches, retail stores, and supermarkets. However, unlike gift cards, they may be used wherever credit cards are accepted.

Functionalities that make prepaid cards attractive to consumers also pose risks for banks that issue prepaid cards and process prepaid card transactions. For example, easy access to prepaid cards, the ability to use them anonymously, and the potential for relatively high volumes

¹ See 31 CFR § 1010.100(ww).

² See Prepaid Access Programs: Risk Management Guidance and Sound Practices; <https://www.occ.treas.gov/news-issuances/bulletins/2011/bulletin-2011-27.html>

of funds to flow through pooled prepaid access accounts, make prepaid cards potentially vulnerable to criminal abuse.³

Contributions

Since prepaid debit and credit cards are readily available and may be used anonymously without generating a record of expenditures, staff believes the use of these cards for campaign contributions should be limited to the same extent as cash contributions. As a result of recent policy changes, ActBlue now automatically rejects contributions that use foreign prepaid/gift cards and domestic gift cards.⁴ Other TPP platforms have also taken steps to prohibit their use for these reasons, and staff has been informed that existing software easily allows for the identification and automatic rejection of contributions from these types of cards. Staff recommends prohibiting the use of prepaid debit and credit cards for all contributions of \$100 or more, consistent with the Act's cash contribution limit of Section 84300(a).

Expenditures

For expenditures of \$100 or more made to a single payee, committees must provide the name and address of the payee as well as the amount and a description of the payment. (Section 84211(k).) Enforcement Division Special Investigators discovered instances where candidates and officeholders provided prepaid debit cards to staffers who used these cards for a variety of purchases, including alcohol, gas, groceries, and food delivery services, with little to no oversight or transparency. As these prepaid cards are not linked to an account, there are no payment records to verify these expenditures. The potential misuse of these prepaid debit cards by staffers is apparent, particularly where prepaid cards in large amounts are at issue, as prepaid cards create an alternative for payments originating from the single designated campaign bank account. Protections need to be put into place to prevent the impermissible use of committee funds by staff members and to hold candidates/officeholders accountable for any misuse of funds. However, staff recognizes that there are legitimate uses for more limited expenditures utilizing prepaid cards, such as the purchase of meals by campaign volunteers.⁵

Proposed Amendments

18430.1. Prepaid Cards, Prohibitions and Limitations on Contributions and Expenditures.

This amendment would prohibit a candidate or committee from purchasing or using campaign funds of \$100 or more for a prepaid debit, prepaid credit, or gift card. In addition, this regulation would prohibit a candidate or committee from accepting any contribution totaling \$100 or more from a single source made with, or consisting of, a prepaid debit, prepaid credit, or gift

³ See FinCEN guide to prepaid cards; <https://www.fincen.gov/sites/default/files/2021-04/Interagency%20Guidance%20to%20Prepaid%20Cards%20508C.pdf>

⁴ <https://republicans-cha.house.gov/2024/12/chairman-steil-releases-findings-from-subpoena-of-actblue>

⁵ These “closed loop” prepaid cards include merchant-specific retail gift cards and mass transit system cards.

card. These cards may be purchased with cash at a wide variety of retailers and lack any associated record of expenditures. This proposed regulation is consistent with the Act's prohibition of cash expenditures of \$100 or more. (Section 84300(b).)

18421.3. Reporting of Contributions and Expenditures Collected by Contract Vendors or Collecting Agents.

This amendment would prohibit candidates or committees from contracting with payment processors that do not utilize AVS to verify and provide the committee with this information along with the corresponding contributions. Third-party payment processors currently collect contributor information in connection with these contributions; this is provided by the contributors and given to the committees for disclosure on campaign statements. This regulation will help to ensure that payment processors utilize industry standard verification protocols and that the committee will also receive these addresses so that they will be able to verify that the information disclosed by the contributors is consistent with that on the cardholder accounts to prevent the laundering of contributions.

18401. Required Recordkeeping for Chapters 4 & 5.

The existing regulation allows for the name, address, and last four digits, or a transaction number. This amendment would require the AVS confirmation of the cardholder's address as part of the original source documentation. This amendment would also bring the record-keeping requirements in line with the amended contract vendor requirement of Regulation 18421.3.

Conclusion

Requiring third-party payment processors to implement AVS protocol and prohibiting all use of prepared debit or credit cards for contributions or expenditures addresses the verification and traceability concerns highlighted by the Enforcement Division Special Investigators, helping to ensure that campaign expenditures are "fully and truthfully disclosed" and that "adequate enforcement mechanisms" exist to verify that expenditures are properly reported.⁶ Further, by ensuring proper identification of potential contributors, this regulation also works to ensure that over-the-limit contributions will not be made or accepted.

Attachments:

Proposed Regulation 18430.1

Proposed Amended Regulation 18421.3

Proposed Amended Regulation 18401

⁶ Section 81002.