BEFORE THE FEDERAL ELECTION COMMISSION
Federal Election Commission
Office of General Counsel
1050 First Street, NE
Washington, DC 20463

In the Matter of:
Complaint Against ActBlue and Associated Entities
366 Summer St, Somerville, MA 02144
Committee ID: **C00401224**
Formed: May 17, 2004

FORMAL COMPLAINT
Pursuant to 52 U.S.C. § 30109(a)(1); 11 C.F.R. § 111.4 and all those cited below.

I. INTRODUCTION

Complainant respectfully submits this sworn and notarized complaint under penalty of perjury pursuant to 52 U.S.C. § 30109, against ActBlue (FEC ID: **C00401224**), and any other associated persons or entities who coordinated, executed, or facilitated violations of the Federal Election Campaign Act of 1971, as amended (FECA), including but not limited to 52 U.S.C. §§ 30122, 30104, 30102, 30109(d), 30109(c), 30116(f), and 11 C.F.R. §§ 110.4(b), 104.3(b), 102.9(a)–(b), 104.3(a)(4), 110.9.

Alleging that Committee **C00401224**, **ACTBLUE**, has processed **178,204,660** or more Smurfed donor transactions, totaling at least **$3,543,266,360**, from up to **281,434** unique Smurfing donors. These transactions account for **39.7%** of the **449,329,799** available committee transactions. The evidence presented here is detailed and thorough, but not exhaustive, and will require further investigation.

At the bottom of this complaint is the document "Informational Notes and Terms" written by Keith Schneider, the owner, developer, and manager of SmurfSearch. It would be helpful for the reader of this complaint to review this executive summary before proceeding.

ActBlue is the largest nonprofit digital platform for donors and functions as a third-party processor for political contributions. It is organized as a PAC with a treasurer responsible for reporting donations to the Federal Election Commission (FEC). The FEC is an independent regulatory agency established to enforce the Federal Election Campaign Act (FECA), which governs campaign financing for U.S. federal offices, including the Presidency, Vice Presidency, House, and Senate. It oversees the public disclosure of funds raised and spent to influence federal elections, including contributions made both to and through ActBlue's platform, even if the amount is less than $1.

ActBlue is also considered a Hybrid PAC defined by the FEC as: "…political committees with non-contribution accounts that solicit and accept unlimited contributions from individuals, corporations, labor organizations, and other political committees to a segregated bank account

for the purpose of financing independent expenditures, other ads that refer to a federal candidate, and generic voter drives in federal elections, while maintaining a separate bank account, subject to all the statutory amount limitations and source prohibitions, that is permitted to make contributions to federal candidates." Essentially, they have two bank accounts: a contribution account and a Non-Contribution Account (or Independent Expenditure-Only Account). This structure allows Hybrid PACs to operate both like a traditional PAC (making direct contributions with limits) and a Super PAC (making unlimited independent expenditures).

On FEC Form 1, Statement of Organization dated 2/17/2023, ActBlue discloses three banks where the committee deposits funds, holds accounts, rents safety deposit boxes, or maintains funds: Citibank (Boston, MA), Bank of America (Washington, D.C.), and Amalgamated Bank (Washington, D.C.).

The current treasurer of ActBlue is George Gilmer. Notably, he failed to understand reporting periods for receipts and desbursements as detailed in Section 104.5(c), as shown by his 1/2/2025 request to the FEC to change ActBlue's reporting dates. His request to the FEC was to switch from a monthly filer to a quarterly filer of receipts and disbursements. The FEC responded to Mr. Gilmer, "Please note that during years that have no scheduled federal election, quarterly filers are required only to file semi-annually."
https://docquery.fec.gov/pdf/227/202501080300234227/202501080300234227.pdf

The statute of limitations for civil enforcement actions under the Federal Election Campaign Act (FECA) is governed by 28 U.S.C. § 2462, which sets a five-year limit for the government to initiate any enforcement action involving a civil fine, penalty, or forfeiture. This Complaint covers the time frame permitted by the FEC under that law. However, the FEC may review earlier activities if they relate to an ongoing scheme or pattern, or if the effects of the violation—such as false reporting, smurfing schemes, or improper filings—continue within the five-year window. In this Complaint, I allege a continuing violation, such as a donor laundering scheme or false reporting spanning from 2015 to 2024. The persistent use of Smurfs indicates ongoing violations of illegal behavior, bringing earlier acts under the scope of current illegal conduct. This is known as the "continuing violation doctrine" in FEC enforcement.

This complaint is brought pursuant to the enforcement provisions of the Federal Election Campaign Act, 52 U.S.C. 30101-30145 (FECA), and related regulations against ActBlue. The evidence primarily pertains to 52 U.S.C. 30122 "Contributions in the Name of Another Prohibited," with supporting evidence suggesting involvement of other related laws outlined below in Section III. §52 U.S.C. 30122 states that "[n]o person shall make a contribution in the name of another person or knowingly permit his name to be used to effect such a contribution, and no person shall knowingly accept a contribution made by one person in the name of another." The Federal Elections Commission (FEC) has implemented this provision at 11 C.F.R. § 110.4(b), which states that no person may "[k]nowingly help or assist any person in making a contribution in the name of another." 11 CFR 110.4(b)(1)(iii). Collectively, these rules and provisions authorize the Commission to investigate ActBlue's acceptance of contributions that—based on pattern, origin, and volume—violate FECA's structural safeguards.

This document:

- presents data supporting an allegation that Committee **C00401224**, **ACTBLUE**, has accepted as many as or more than **178,204,660** Smurfed donor transactions totaling at least **$3,543,266,360** from as many as **281,434** unique Smurfing donors. These transactions account for **39.7%** of the **449,329,799** available committee transactions and represent **29.3%** of the **$12,075,259,871** total committee transaction value.
- provides evidence supporting the assertion that ActBlue may have violated the Federal Campaign Act of 1971, as amended (FECA), including but not limited to 52 U.S.C. 30122 and 11 C.F.R. § 110.4(b), by laundering money not only into their PAC but also by offering a portal to inject illicit funds into the committees that use their platform.
- exposes how the FEC deliberately excluded at least 538 million uncoded (or uncategorized) transactions, with an Entity Type of IND (individual), totaling over $10 billion that have been hidden from effective oversight—more than twice the number of categorized receipts the FEC provides in their bulk download for researchers. The FEC blames committees for sloppy reporting as a reason to withhold these transactions. Included in these was **388,748,632** ActBlue uncoded transactions—87% of ActBlue individual transactions—not included in the bulk download.
- Details how SmurfSearch shows ActBlue recorded $12,075,259,870 in individual donor receipts to the FEC, but it's hard to trace where the money was allocated, and the figures don't add up.
- outlines poor and/or intentional reporting standards demonstrated by ActBlue, showing how ActBlue's reports of incoming donations to the FEC lack uniformity and consistency by not applying transaction codes and standard memo texts, which obscure the source and intent of a transaction. These matters in question also include allowing **462,147** transactions with indeterminate zip codes and using state codes that do not exist because ActBlue, seemingly deliberately, bypassed address verification systems.
- displays strong evidence showing that ActBlue reports potential artificially created contributors and their identifying details to the FEC by using uncommon first names and surnames, indicating the use of synthetic name generation, a common Smurfing tactic.

What is Political Smurfing

Smurfing is a form of structured money laundering where criminals divide large sums of money into smaller transactions to avoid regulatory reporting and hide the origins of illegal funds. In the context of political Smurfing, individuals whose identities are stolen, known as Smurfs (also called Straw Donors), are used as donors to distribute these smaller transactions to both state and federal committees. These individuals are typically over 65, listed as retired, not employed, unemployed, or have unknown occupations, or a combination of these in the same FEC statement. Smurfed contributions are made in their names without their knowledge or consent. This practice harms all U.S. citizens by undermining trust in the election process, public institutions, and the information environment, especially within political and grassroots campaign efforts. Smurfing is a serious crime that violates state and federal campaign finance laws.

The question has been asked repeatedly, "why Smurf money into campaigns with individual donations when one can make unlimited contributions to certain PACs, which will then contribute to candidates?" The answer is, "why not do both?" The tactic of "astroturfing" campaigns and PACs—loading them with illicit individual contributions—helps create the illusion of widespread support while hiding the source of the funds. Even small donations from donors from diverse backgrounds across every state can boost public support and fill up coffers.

Definition of "to and through ActBlue"

Throughout this complaint, the phrase "to and through ActBlue" is frequently used. This refers to direct donations to ActBlue (to), as well as earmarked donations processed through ActBlue (through). When donating to a committee via ActBlue, you can choose to give directly or split your donation between ActBlue itself and other committees or causes. ActBlue offers a feature called "Split It!" that allows you to divide a single contribution among multiple recipients (known as earmarking). A donor can specify how much they want to give to each recipient or opt not to contribute to certain listed committees. For example, you might donate to any or all Democratic committees or organizations and also decide to allocate part of your donation to ActBlue to support their fundraising platform. ActBlue, as a conduit, then forwards the earmarked donations to the intended recipients.

Data Sources and Effects of Missing Uncoded Transactions

The Smurfing issues raised in this complaint are based on thorough analysis by independent investigators of data from the United States Federal Election Commission (FEC) website, which includes individual transactions recorded by campaign and committee treasurers. This data was exported and logically organized in SmurfSearch (https://smurfsearch.electionwatch.info/menu.php), allowing the investigation of **449,329,799** transactions made to and through ActBlue.

To be more specific, SmurfSearch used FEC data to compile contributor transactions that spans **10.25 years from 2015 through July 14, 2025.** Data acquired from the following sources results in a total SmurfSearch database of **801,273,628** transaction records:

- The FEC website offers publicly available bulk download zip files for each two-year cycle published as 2016, 2018, 2020, 2022, 2024, and 2026 (last downloaded July 14, 2025). These datasets total approximately 262,929,275 million records. The FEC explicitly states that they are to be used for reasons, among others, public analysis.
- FEC's weekly internal database backup was acquired from the AWS (Amazon Web Services) Cloud using a URL provided by FEC Technical Support Staff. The backup used for constructing the database was downloaded on May 19, 2025. It was restored to a server. Within this database, a large number of transaction records without a transaction type code were identified. Approximately **602 million** of these records were extracted, covering the date range from 01-01-2015 to the most recent available, which is May 19, 2025.

The SmurfSearch website shows that ActBlue's data is inconsistent and lacking integrity, which makes the FEC data unreliable. Among other issues, 87% of ActBlue transactions lack

transaction type codes, allowed by the FEC, and **462,147** transactions have indeterminate zip codes and state codes.

An affidavit from a SmurfSearch researcher/programmer, Greg Sternbach, an IT Technician and Data Infrastructure Engineer, was submitted confirming that "In June 2025, SmurfSearch researchers found that there were over 500 million donations with blank transaction type codes missing between 2015 and 2025 while examining individual donor details in the bulk downloaded transactions from the FEC public website. These totals could not be reconciled with the bulk data downloads loaded into SmurfSearch (a website that helps expose how money is laundered into political campaigns). When questioning the FEC support staff about this discrepancy, the FEC stated that the transaction type code field is not required on filing forms for donations under $200. Only transactions with properly filled-in transaction type codes are included in the bulk data files available for download from the FEC website. The FEC explained that it is on purpose to align with all historical campaign donation data back to 1975. To get all donation transactions, the FEC staff recommended downloading the full raw database dump backup files from the Amazon S3 bucket (a cloud-based storage for the FEC database backup data). The backup storage is open to the public to analyze all donations, including those with "blank" transaction type codes. These are also known as uncategorized transactions. Downloading and assembling the raw database requires significant computer processing power and database expertise to accurately build and access the complete database for analysis".

Please see the affidavit and "Informational Notes and Terms" at the end of this document for additional details.

See 6/26/25announcement at:
https://smurfsearch.electionwatch.info/db872siteupgrade_dashboard.php

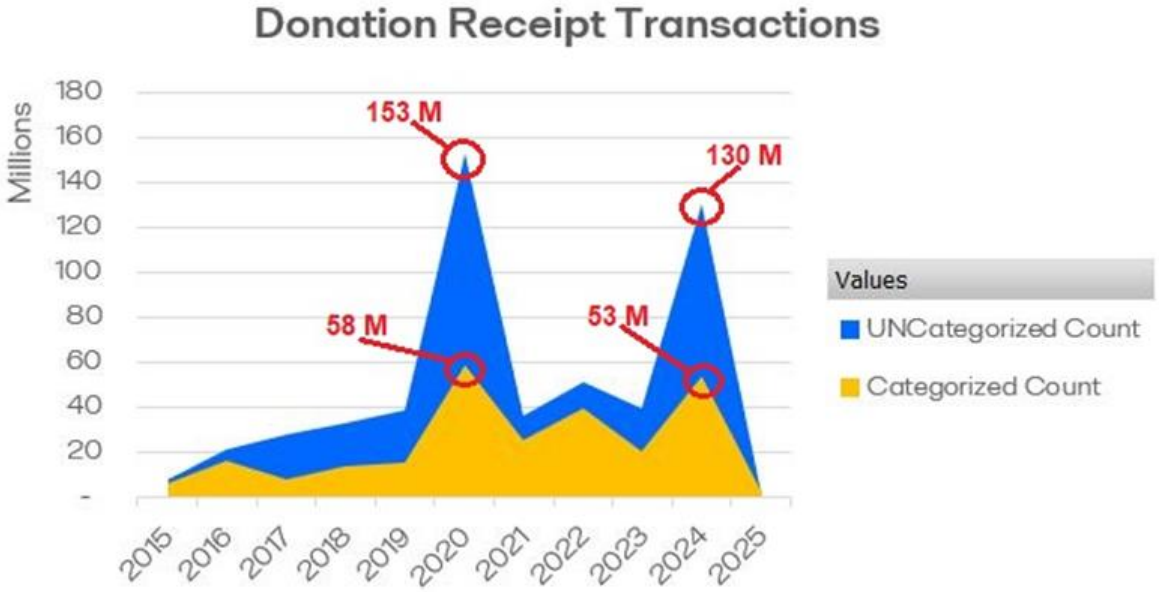
Attn: DOJ, FBI and Committee on House Administration. The Federal Election Commission (FEC) is failing to close a loophole to protect our federal and state elections from the money laundering scheme called **SMURFING**. This practice thrives in the shadows of the FEC, an independent agency of the U.S. Government that is supposed to administer and enforce federal campaign finance laws. Bulk data the FEC provided to researchers for the past several years had 500+ million uncoded (or uncategorized) transaction receipts deliberately excluded. That's over 200% of all donor transactions totaling over $10 billion!

Smurfing works by breaking large, illegal donations into small, seemingly legitimate ones, often funneled through real life unsuspecting intermediaries who are largely aged 65 and older. Without a receipt type, these transactions are nearly impossible to track systematically in the bulk data available for download from the FEC website. Want to investigate all transactions recorded at the FEC? You're stuck using the throttled OpenFEC API or manually downloading donor records one by one from the website—impractical for exposing mass fraud. The FEC blames committees for sloppy reporting, but this loophole is no accident.

Committees know uncategorized receipts won't make it into bulk files, shielding suspicious activity from scrutiny.

Here's the problem: the FEC's bulk data downloads used by researchers to analyze donation trends only include transactions with categorized receipt types. The FEC allows political committees to leave the receipt type field blank—it's optional on reporting forms which creates a blind spot. Thousands of committees exploit this, submitting uncategorized receipts that vanish from bulk data files making them the perfect vehicles for smurfing.

Since 2015, over 500 million uncategorized receipt transactions have been obscured from effective oversight, over twice as many as the categorized receipts resulting in over 10 BILLION shadow campaign dollars hidden from the public. This is fueling the growing smurfing epidemic that erodes public trust in our elections and turns honest elections into corrupt selections. The FEC's own rules show transaction codes are meant to help group activities, but they're not enforced. For donations over $200, occupation and employer are required, yet for smaller, uncategorized donations, even basic donor details can be missing. Every uncategorized receipt should raise red flags, but the FEC's hands-off approach lets smurfing flourish. In the uncategorized vs categorized receipt type chart below, you can see obvious smurfing trends with the uncategorized transactions.



When comparing ActBlue individual contributions listed in the table below since 2004 from the FEC website, it is notable that the increase in uncategorized transactions shown in the table above in 2020 coincides with the highest total ActBlue recorded receipts of $4,318,377,981.32,

and again in 2024 for the second-highest total of $3,821,173,165.20. This further indicates that the FEC's loophole of not requiring transaction codes allows committees to bypass recording receipt type codes, making these transactions invisible in bulk data downloads and possibly shielding smurfing fraud from scrutiny. The lack of transparency acts as a shield, making detection and accountability more difficult, and may enable illicit funds and stolen identities to repeatedly enter the donor system. This isn't sloppy reporting; it is a deliberate blind spot that fuels corruption. Billions of dollars in campaign funds lack transparency, turning elections into selections. This poses a major threat to our Democratic Republic, unlike anything we have seen before.

ActBlue History of Individual Contribution Totals Reported by the FEC			
Coverage dates	**Total Receipts**	**Total Contributions**	**Total Ind Contributions**
01/01/2025 to 06/30/2025	$519,983,799.66	$505,066,827.51	$505,066,827.51
01/01/2023 to 12/31/2024	$3,821,173,165.20	$3,758,627,950.83	$3,758,627,950.83
01/01/2021 to 12/31/2022	$2,227,362,047.76	$2,188,544,235.41	$2,188,544,235.41
01/01/2019 to 12/31/2020	$4,318,377,981.32	$4,243,096,496.78	$4,243,096,496.78
01/01/2017 to 12/31/2018	$1,261,994,019.93	$1,236,251,823.46	$1,236,251,823.46
01/01/2015 to 12/31/2016	$694,740,214.79	$679,908,044.18	$679,908,044.18
01/01/2013 to 12/31/2014	$280,314,315.83	$276,701,106.20	$276,701,106.20
01/01/2011 to 12/31/2012	$151,119,903.54	$149,694,686.09	$149,694,686.09
01/01/2009 to 12/31/2010	$63,970,125.25	$63,235,415.26	$63,235,415.26
01/01/2007 to 12/31/2008	$54,598,569.95	$53,349,246.96	$53,349,246.94
01/01/2005 to 12/31/2006	$15,979,985.34	$15,935,339.66	$15,935,339.66
04/01/2004 to 12/31/2004	$914,033.86	$911,934.40	$911,934.40
Totals	**$13,410,528,162.43**	**$13,171,323,106.74**	**$13,171,323,106.72**

Who Uses the ActBlue Platform

Since 2004, $17 billion has been raised through ActBlue, according to its own website. ActBlue manages the processing and disbursement of earmarked donations from individual contributions made via its digital platform for candidates, committees, and contributions to its own platform. It claims to have implemented internal measures to ensure compliance and detect fraud. ActBlue has never been audited by the FEC, holding them all accountable for increasing the risk of fraud, errors, and loss of public confidence.

The following is a link listing 8,520 committees and organizations that use ActBlue as their fundraising platform: https://secure.actblue.com/directory/all/org/D?focus_area=Environment&page=78. It claims that over **23 million** people have donated through ActBlue and that **15 million** ActBlue Express users have saved their contact and payment information, enabling contributors to make one-click donations easily.

A Politico article dated 10/30/2020 quoted Erin Hill, then-ActBlue's executive director, saying, "Small-dollar donors are funding everything — 21,000 different candidates and committees and causes — because it's that kind of scope that involves our democracy." (https://share.google/7I69jbYopp7e60s5Q) The article also mentions that "ActBlue is used by a wide range of high-profile Democratic committees and campaigns, including the Democratic National Committee (DNC), the Democratic Senatorial Campaign Committee (DSCC), the Democratic Congressional Campaign Committee (DCCC), the Democratic Governors Association (DGA), and the Democratic Legislative Campaign Committee (DLCC)."

FEC ActBlue Audit and Investigation History

At the FEC, by law, all enforcement cases must remain confidential until they're closed. There are 1,066 audit reports from 1976 to 2022 on the FEC website: https://www.fec.gov/legal-resources/enforcement/audit-search/. ActBlue or any of its affiliates are not listed among the audit reports.

The Office of Inspector General submitted a report on 11/13/24 titled "Management and Performance Challenges Facing the FEC for FY 2025" https://www.fec.gov/resources/cms-content/documents/FY-2025-Mgmt-Challenges.pdf, stating that "The FEC receives campaign finance reports, statements and other disclosure documents from more than 16,000 political committees and other filers" and identified "the top management and performance challenges facing the Commission as the following: • Budget • Modernization of information systems and cybersecurity • Growth of election contributions • Outdated statutory pay structure".

Recent reports indicate the agency is paralyzed without a quorum. Currently, there are only 3 commissioners on staff, with three vacancies. FECA requires at least four agreeing votes to decide on issues such as investigation outcomes, citing committees for campaign finance violations, issuing advisory opinions, or guidance for campaigns.

The following reports call for investigations against ActBlue:

- President Trump signed a memo On April 24, 2025 targeting ActBlue, a major Democratic Party donor platform, as part of an effort to investigate potential illegal campaign donations. https://www.whitehouse.gov/fact-sheets/2025/04/fact-sheet-president-donald-j-trump-investigates-unlawful-straw-donor-and-foreign-contributions-in-american-elections/

- The Committee on House Administration (CHA), which oversees FEC operations, is well aware of ActBlue's criminal activity. Two press releases were issued very recently. This particular one https://judiciary.house.gov/media/press-releases/fraud-actblue-new-report-details-potential-illegal-activity-democrat-platform#:~:text=WASHINGTON%2C%20D.C.%20%E2%80%93%20Today%2C%20the,for%20Illegal%20Election%20Contributions.%22%20This cited: "Internal documents show that ActBlue executives and staff are aware that both foreign and domestic fraudulent actors are exploiting the platform but do not take the threat seriously. In fact, they attempted to hide the changes to avoid sparking discussions about fraud on the platform. For example, ActBlue's training guide for new fraud-prevention employees instructed them to "look for reasons to accept contributions," rather than err on the side of flagging suspicious donations. Internal communications further reveal that, rather than seeking to reduce or eliminate fraud, ActBlue's chief fraud-prevention official was willing to accept 10 percent more fraud while focusing on DEI. Additionally, in a thirty-day window during September and October 2024, ActBlue detected 237 separate donations made from foreign IP addresses using domestic prepaid cards."

  The following lines were taken from this press release: https://cha.house.gov/2025/7/chairmen-steil-jordan-and-comer-subpoena-documents-from-actblue-ceo#:~:text=Background:,preventing%20foreign%20and%20illegal%20contributions. CHA is concerned that ActBlue has *"accepted fraudulent donations from domestic and foreign sources"*. It goes on: "On April 2, 2025, the Committee on House Administration, the House Judiciary Committee and the House Committee on Oversight and Government Reform **released a joint interim staff report** that revealed ActBlue made its fraud-prevention rules "more lenient" twice in 2024—even though there is extensive fraud on the platform, including from foreign sources". Then "On November 27, 2023, **ActBlue responded** to Chairman Steil's letter saying it did not require a CVV in order to contribute on their website". Then, "On June 25, 2025, Chairmen Steil, Comer and Jordan **issued two subpoenas**, to a current and a former ActBlue employee, after they both failed to comply with the Committees' request for transcribed interviews". That ActBlue employee is Regina Wallace-Jones, CEO and President of ActBlue. Banks have filed thousands of suspicious activity reports against ActBlue that have been ignored, but now must be addressed.

- "A sprawling investigation into the online fundraising platform ActBlue has expanded into 19 states, as attorneys general across the country press the company on its security practices and whether Democrats might be using the platform to cheat on election donations." https://amac.us/newsline/politics/newsline/politics/probe-into-whether-democrats-use-actblue-platform-to-cheat-at-fundraising-expands-to-19-states/

- Darrell Issa, A top lawmaker, on March 12, 2025 asked the Trump administration to investigate "credible allegations" that ActBlue, the Democratic fundraising platform, violated federal law in allowing terrorism-linked groups to use its services. https://issa.house.gov/media/in-the-news/icymi-issa-calls-investigation-actblue

- Sen. Mark Finchem appeared on Newsmax in August, 2025 to discuss what he calls a massive money laundering scheme involving ActBlue, the Democratic fundraising platform. He claims the Election Fairness Institute uncovered a long-running operation using inflated, off-the-books mortgage transactions—what he calls "magic mortgages"—to funnel hundreds of billions of dollars into U.S. politics. Finchem suggests the funds come from foreign actors, including BRICS nations, aiming to influence American elections. https://votefinchem.com/mark-finchem-on-newsmax-magic-mortgage-money-laundering-scheme-tied-to-actblue/

- Ken Paxton, Attorney General of Texas, submitted a letter to Lisa J. Stevenson, Acting General Counsel to the FEC on 10/21/2024 re: Petition for the Issuance and/or Amendment of Rules Regarding Contributions from Untraceable Electronic Payment Methods. One paragraph summarizes their concern: "Notably, however, one of the most prominent online contribution platforms—ActBlue— submitted comments to the Commission encouraging it not to adopt regulations for prepaid cards that would have hampered this potential fraud. In those comments, ActBlue made representations about important technological realities that, as explained below, are no longer accurate (if they ever were). Moreover, the Attorney General's findings cast serious doubt on ActBlue's representation that "prepaid cards likely present less of a risk" of unlawful contributions "than cash does."4 It appears that the opposite is true—prepaid cards present a far greater risk". https://www.texasattorneygeneral.gov/sites/default/files/images/press/ActBlue%20FEC%20Petition%20Redacted%20Final.pdf

II. FACTUAL ALLEGATIONS

A. Mechanics and Exploitation of Political Smurfing

On November 27, 2023, **ActBlue responded** to Chairman Steil's letter, stating that they do not require CVV codes for contributions on their website. Keep in mind that, as noted above, Politico reported that "21,000 different candidates and committees and causes" use the ActBlue platform. The Committee on House Administration reported that ActBlue's internal documents show that ActBlue executives and staff are aware that both foreign and domestic fraudulent actors are exploiting the platform but do not take the threat seriously. In fact, they attempted to hide the changes to avoid sparking discussions about fraud on the platform. For example, ActBlue's training guide for new fraud-prevention employees instructed them to "look for reasons to accept contributions," rather than err on the side of flagging all suspicious donations. Internal communications further reveal that, rather than seeking to reduce or eliminate fraud, ActBlue's chief fraud-prevention official was willing to accept 10 percent more fraud while focusing on DEI. This may leave the 21,000 or more committees or organizations who use the ActBlue fundraising platform vulnerable and without any safeguards against bad actors. Alternatively, these committees and/or organizations might be involved in a coordination of political collusion.

Additionally, local, state, and federal treasurers serve as the electronic filers for their committees and organizations. They often use Excel or can request ActBlue software or other dedicated donor management software to simplify record-keeping, which is then transferred, mostly

electronically, to the FEC and state oversight agencies. Treasurers often begin by using Excel or specialized donor management software to manage and organize contribution and expenditure data from various sources, including receipt records from platforms like ActBlue. This helps them track and compile data, especially for contributions that reach the $200 threshold, which requires recording the contributor's occupation and employer. This information is then imported into specialized reporting software like FECFile or through platforms with built-in reporting features that help prepare reports in the format required by the FEC. The final report generated by the software is submitted electronically to the FEC. It's also worth noting that reports indicate treasurers do not always report the conduit if a donation was received through one.

Understanding how treasurers organize their contribution data can expose vulnerabilities that enable the injection of illicit donations. For instance, campaign workers might, under the pretense of collecting donor information and credit card details at fundraising events, through campaign letter invitations, or via remittance cards, launder money using Smurfs. They do not process the donations at the event; instead, they can claim they take the information back to the office and record it in the donor portal on their campaign website. What's to stop a malicious actor from stealing identities and using prepaid or gift cards, inputting false or laundered money into their campaign portal, recording it on their Excel spreadsheets or other donor management software, and submitting it to the FEC? There has reportedly not been a treasurer who has stepped forward to report possible illegal activity resulting from receiving unusual, high-volume, micro-structured political contributions from their fundraising platform. Receiving questionable donations isn't as important as winning.

Recently, Senator Fincham exposed the Magic Mortgage Scandal, where ActBlue is involved in a nationwide real estate mortgage scandal to funnel illegal funds into Democrat-aligned PACs and NGOs via ActBlue platform. If you control the system, it is easy to manipulate and corrupt it.

Regarding coding donation transactions, while reviewing "Getting Started with FECFile User Manual Hands-on Help with FECFile and Electronic Filing for Candidate Committees," it was found that it does not instruct a treasurer on how to implement the transaction codes provided by the FEC. In fact, it doesn't mention transaction codes at all. More on individual transaction codes will be discussed below.

ActBlue has raised over $17 billion through its platform since 2004. The following is a link listing 8,520 committees and organizations that use ActBlue as their fundraising platform: https://secure.actblue.com/directory/all/org/D?focus_area=Environment&page=78. It claims that over 23 million people have donated through ActBlue and that **15 million** ActBlue Express users have saved their contact and payment information, enabling contributors to make one-click donations easily. Like most donation platforms, once a credit card, gift card, or debit card is used, you may only be asked for your CVV the first time you use it, if at all. As mentioned above, ActBlue admitted not requesting CVV codes. Considering SmurfSearch has identified 281,434 possible unique ActBlue Smurfs over 178,204,660 transactions, is ActBlue verifying CVV codes from "donors" who are currently donating but have been on record for the last 10 years or more, or are they allowing past donors to go unchecked?

Payment Card Industry Data Security Standard (PCI DSS) strictly prohibits storing CVV codes after transaction authorization for any reason, including card-on-file or recurring transactions. All merchants that accept, store, or transmit cardholder data must comply with PCI DSS

requirements. A credit card CVV does not link the card back to a specific person or their bank like a PIN does; rather, it is a security code used by merchants to verify that the cardholder has the physical card during a "card-not-present" transaction. The CVV is a unique number generated by the card issuer, which is usually a bank or financial institution. **Credit card networks can also act as issuers, providing credit directly to consumers without a traditional bank [emphasis added].** By requiring users to re-enter the CVV code for repeat donations, ActBlue can ensure that sensitive data is not stored on its servers, helping maintain compliance with industry standards. However, this does not go far enough to prevent fraud, like Smurfing. A comprehensive audit would reveal whether ActBlue's credit card infrastructure meets PCI DSS standards, as well as examine "audit trails," which would chronologically record all activity and transactions used to detect suspicious patterns and prevent identity theft.

SmurfSearch generates reports on over 2,000 committees with high Smurf activity. Among them are the Democratic National Committee (DNC), the Democratic Senatorial Campaign Committee (DSCC), the Democratic Congressional Campaign Committee (DCCC), Progressive Turnout Project, and End Citizens United—all listed on the ActBlue website—the platform for 8,520 committees and organizations a donor can contribute to in one place https://secure.actblue.com/directory/all/org/D?focus_area=Environment&page=78. This portal offers a significant opportunity for bad actors to use algorithms to add fake donors, potentially indicating systematic political collusion and fraud. If someone controls the system, it can be easily manipulated and corrupted at will.

Below are snapshots of SmurfSearch data for five out of 8,520 committees and organizations listed on the ActBlue donor website, which is paid for by ActBlue. Highlighted are the numbers of alleged unique Smurf donors and the total Smurfed dollars.

		Trx All Cnt	Trx All Amt$	Unique Smurfs
C00010603 Committee WASHINGTON,DC, FEC Cmte Info	DNC SERVICES CORP./DEM. NAT'L COMMITTEE	1,259,174	$125,988,670	63,973
		P: 1,259,017	P: $126,911,708	
		N: 157	N: ($923,038)	

Cmte ID etc.	Cmte Name	Trx All Cnt	Trx All Amt$	Unique Smurfs
C00042366 Committee WASHINGTON,DC, FEC Cmte Info	DSCC	2,145,123	$197,327,979	93,770
		P: 2,145,062	P: $197,372,315	
		N: 61	N: ($44,336)	

Cmte ID etc.	Cmte Name	Trx All Cnt	Trx All Amt$	Unique Smurfs
C00000935 Committee WASHINGTON,DC, FEC Cmte Info	DCCC	4,212,088	$227,195,637	105,729
		P: 4,202,299	P: $243,378,500	
		N: 9,789	N: ($16,182,863)	

Cmte ID etc.	Cmte Name	Trx All Cnt	Trx All Amt$	Unique Smurfs
C00580068 Committee NORTHBROOK,IL, FEC Cmte Info	PROGRESSIVE TURNOUT PROJECT	1,822,905	$45,571,903	48,921

Cmte ID etc.	Cmte Name	Trx All Cnt	Trx All Amt$	Unique Smurfs
C00573261 Committee WASHINGTON,DC, FEC Cmte Info	END CITIZENS UNITED	1,729,067 P: 1,714,319 N: 14,748	$42,628,804 P: $43,525,294 N: ($896,491)	43,229

B. Transaction Type Codes

ActBlue collects information about donors, such as their name, address, contribution amount, date of contribution, and, if the total exceeds $200 per election cycle, their occupation and employer, as required by federal campaign finance laws. The FEC provides a list of transaction codes for each transaction type, whether it is a direct contribution, an earmarked contribution, earmarked treasury out, or other categories. The following are common FEC transaction codes used to classify Entity Type "Individual" transactions.

Code Type	Description
10	Contribution to Independent Expenditure-Only Committees (Super PACs), Political Committees with non-contribution accounts (Hybrid PACs) and nonfederal party "soft money" accounts (1991-2002) from a person (individual, partnership, limited liability company, corporation, labor organization, or any other organization or group of persons)
15	Contribution to political committees (other than Super PACs and Hybrid PACs) from an individual, partnership or limited liability company
15E	Earmarked contributions to political committees (other than Super PACs and Hybrid PACs) from an individual, partnership or limited liability company
20Y	Nonfederal refund
22Y	Contribution refund to an individual, partnership or limited liability company
24T	Earmarked contribution passed to intended recipient from intermediary's treasury (treasury out)

ActBlue is a Hybrid PAC. It is classified as a "PAC with Non-Contribution Account," meaning it operates as both a traditional PAC and a Super PAC. This enables ActBlue to accept both limited and unlimited contributions. Reviewing the FEC's 106 Transaction type codes, there is no specific code assigned to donations to Hybrid PACs like ActBlue. When ActBlue records donations made directly to them to support their platform, they either use code 15, which is intended for "contributions to political committees other than Super PACs and Hybrid PACs," or they do not assign a code at all. To make matters more confusing, ActBlue sometimes uses codes 10, 15E, 24T, or uncoded transactions interchangeably. As a result, it is impossible for the public

to identify and verify all donation types to and through ActBlue. The lack of transparency is striking.

Here are the statistics collected by SmurfSearch on ActBlue code type counts:

<prev - next> ID: C00401224 -- ACTBLUE						
FEC Transaction Types - Committee Stats vs: Smurfs Stats						
https://www.fec.gov/campaign-finance-data/transaction-type-code-descriptions/						
FEC Trx Type	**Committee All Trx Data**		**Smurfs Only Collected Trx Data**			
	Trx Count	**Trx Amount**	**Trx Count**	**Cmte%**	**Trx Amount**	**Cmte%**
	388,748,632	$6,070,226,651	138,576,845	**35.60 %**	$1,637,446,881	**27%**
15	9,725,826	$67,089,744	9,142,308	**94%**	$40,321,499	**60.10 %**
15E	400	$249,116	144	**36%**	$78,919	**31.70 %**
20Y	19	$2,982	9	**47.40 %**	$127	**4.30%**
22Y	277,653 P: 277,508 N: 145	$3,970,936 P: $3,996,663 N: ($25,727)	119,869 P: 119,816 N: 53	**43.20 %**	$1,522,372 P: $1,538,942 N: ($16,570)	**38.30 %**
24T	50,577,269 P: 49,222,990 N: 1,354,279	$5,933,720,441 P: $6,106,378,827 N: ($172,658,386)	30,365,485 P: 29,781,825 N: 583,660	**60%**	$1,863,896,562 P: $1,931,195,050 N: ($67,298,488)	**31.40 %**
Totals:	**449,329,799** **P: 447,975,375** **N: 1,354,424**	**$12,075,259,870** **P: $12,247,943,983** **N: ($172,684,113)**	**178,204,660** **P: 177,620,947** **N: 583,713**	**39.70 %**	**$3,543,266,360** **P: $3,610,581,418** **N: ($67,315,058)**	**29.30 %**

Most notably:
- Out of **449,329,799** ActBlue transactions, **388,748,632,** totaling over **$6 billion,** are not coded. There are memo texts that indicate whether it is a donation to ActBlue, an earmarked donation, or various other descriptions that are obscure and inconsistent.
- **94%** of donations, totaling **$40,321,499,** originated from suspected Smurfs. When ActBlue assigns a code with a 15 to transactions, the money is transferred directly to the intended recipient, who is almost always ActBlue. A forensic audit would be needed to determine how many of the uncoded transactions in the uncoded bucket also went to ActBlue.
- **60%** of donations coded as 24T, totaling **$1,931,195,050,** came from suspected Smurfs. These are earmarked donations, and ActBlue forwarded these contributions to the designated recipients (treasury out).
-**$3,970,936** in ActBlue refunds coded as 22Y are contribution refunds and should be recorded as expenditures on FEC Schedule B. These transactions ActBlue maybe recorded incorrectly on Schedule A for itemized receipts and, therefore, are included in the bulk download, which explains why they appear in SmurfSearch.

The FEC provides a search feature on its Advisory Opinions webpage. https://www.fec.gov/press/resources-journalists/advisory-opinions/#:~:text=Advisory%20opinions%20are%20official%20Commission,complete%20description%20of%20the%20process. An FEC advisory opinion (AO) is an official response from the FEC answering questions about how federal campaign finance law applies to specific situations. Essentially, it is the FEC's way of offering guidance on the legality of proposed actions under the law. The following, written on September 25, 2014, is **AO 2014-13: Contributions earmarked for multiple committees.** https://www.fec.gov/updates/ao-2014-13-contributions-earmarked-for-multiple-committees/ This particular AO addressed whether "Contributors may use ActBlue's "Split It!" feature on its contribution forms to divide a single contribution among multiple political committees, including candidate committees. Using this feature will not result in ActBlue exercising direction or control over the choice of recipient candidates or political committees, nor will it trigger the Commission's joint fundraising rules." It also states, "Any person who receives and forwards an earmarked contribution to a candidate is considered a "conduit or intermediary." 11 CFR 110.6(b)(2). A forwarded earmarked contribution does not count against the conduit's contribution limits unless the conduit "exercises any direction or control over the choice of the recipient candidate." **If the conduit exercises direction or control, then the entire earmarked contribution is treated as a contribution from both the original contributor and from the conduit to the recipient candidate. 11 CFR 110.6(d). [emphasis added]"** Although the FEC didn't comment on transaction code 24T, the bolded sentence seemingly explains why ActBlue uses the FEC-provided transaction code 24T (when they do assign codes), as the FEC seems to permits treasurers to categorize an earmarked donation as a 24T "Earmarked contribution passed to the intended recipient from intermediary's treasury (treasury out)." This suggests that all recorded 24T's are individual contributions and are not counted twice—once as a contribution and once as treasury out to the intended recipient.

Research shows that the FEC does not strictly enforce the use of transaction codes, even when they are provided to each committee. Why does ActBlue sometimes use these codes but mostly not, given the evidence of the uncoded 388,748,632 transactions? The Federal Election Campaign Act (FECA) requires committees to maintain detailed, structured internal records for reporting, but it can't be found that they mandate the same level of detail when reporting contributions to the FEC. This inconsistency in classifying financial transactions into different categories makes it difficult to trace the true source and purpose of funds.

ActBlue serves as a pass-through for earmarked contributions. ActBlue must forward the earmarked contribution to the recipient candidate committee within 10 days of receiving the contribution. Besides reporting earmarked donations to the FEC on the relevant report, ActBlue also provides a special transmittal report to the authorized committee receiving the contribution. This report includes all the information the candidate committee needs for its records and for reporting to the FEC, as well as for the receiving committee. When digitally submitting recorded transactions to the FEC website, ActBlue rarely uses the transaction codes provided by the FEC. Doesn't this inconsistency raise red flags and trigger an audit? According to its records, the FEC has never audited ActBlue.

To elaborate on this criticism, instead of using transaction codes, ActBlue typically relies on memos in the provided memo text column. ActBlue's memos are often vague, inconsistent, and incomplete. A typical example from a single donor, Sonia Immasche from Colorado, shows a few transaction lines from her FEC records. Notice the absence of transaction codes in the receipt_type column. Additionally, there is arbitrary writing in the memo texts, such as [MEMO ITEM], #NAME, and *.

contributor_id	receipt_type	receipt_type_desc	receipt_type_full	memo_text
C00782599	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR ELECT DIVERSE DEMOCRATS PAC (C00782599)
			EARMARK	EARMARKED FOR END CITIZENS UNITED PAC (C00573261)
	15	CONTRIBUTION		
	10	NON-FEDERAL RECEIPT FROM PERSONS		* EARMARKED CONTRIBUTION: SEE BELOW
	10	NON-FEDERAL RECEIPT FROM PERSONS		* EARMARKED CONTRIBUTION THROUGH ACTBLUE ON 09/24/2020
				*
				[MEMO ITEM] *
	15E	EARMARKED CONTRIBUTION		NSF - EARMARKED THROUGH ACTBLUE
	15E	EARMARKED CONTRIBUTION		NSF - EARMARKED THROUGH ACTBLUE
C00401224	15E	EARMARKED CONTRIBUTION		NSF - EARMARKED THROUGH ACTBLUE
				#NAME?
				[MEMO ITEM] *
				*
				[MEMO ITEM] *
			CONTRIBUTION TO ACT BLUE	
			CONTRIBUTION TO ACT BLUE	
C00401224	15E	EARMARKED CONTRIBUTION		* EARMARKED CONTRIBUTION: SEE BELOW
C00401224	15E	EARMARKED CONTRIBUTION		* EARMARKED CONTRIBUTION: SEE BELOW
C00401224	15E	EARMARKED CONTRIBUTION		* EARMARKED CONTRIBUTION: SEE BELOW
	15	CONTRIBUTION		
C00401224	15E	EARMARKED CONTRIBUTION		* EARMARKED CONTRIBUTION: SEE BELOW
			EARMARK	EARMARKED FOR END CITIZENS UNITED PAC (C00573261)
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
C00748228	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR MARCH ON PAC (C00748228)
			EARMARK	EARMARKED FOR BECCA BALINT FOR VERMONT (C00797175)
C00845164	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR TEKESHA MARTINEZ FOR CONGRESS (C00845164)

	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
C00580068	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR PROGRESSIVE TURNOUT PROJECT (C00580068)
			EARMARK	EARMARKED FOR TERRI SEWELL FOR CONGRESS (C00458976)
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
			EARMARK	EARMARKED FOR 314 ACTION FUND (C00633248)
			EARMARK	EARMARKED FOR TURN LEFT PAC - INDEPENDENT EXPENDITURE (C00839894)
			EARMARK	EARMARKED FOR EQUALITY PAC (C00550970)
C00748228	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR MARCH ON PAC (C00748228)
			EARMARK	EARMARKED FOR BECCA BALINT FOR VERMONT (C00797175)
C00845164	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR TEKESHA MARTINEZ FOR CONGRESS (C00845164)
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
C00580068	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR PROGRESSIVE TURNOUT PROJECT (C00580068)
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
			EARMARK	EARMARKED FOR TERRI SEWELL FOR CONGRESS (C00458976)
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
C00748228	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR MARCH ON PAC (C00748228)
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
C00651042	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR MOMS FED UP (C00651042)
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
	15	CONTRIBUTION	CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
C00550970	24T	EARMARKED INTERMEDIARY TREASURY OUT	EARMARK	EARMARKED FOR EQUALITY PAC (C00550970)
			EARMARK	EARMARKED FOR EQUALITY PAC (C00550970)
			EARMARK	EARMARKED FOR ROSEN FOR NEVADA (C00606939)
			EARMARK	EARMARKED FOR JEFFRIES FOR CONGRESS (C00503052)
			CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE
			CONTRIBUTION TO ACT BLUE	CONTRIBUTION TO ACTBLUE

The FEC provides transaction codes to categorize and classify financial activities. This is important because mis-categorizing or not categorizing transactions can distort their source and hide details, making auditing nearly impossible since they lay the foundation for tracking transactions and creating a clear audit trail. Essentially, coding transactions adds structure and order to financial data, making it easier to record, manage, analyze, and report a committee's financial activities. This, in turn, promotes greater transparency, accuracy, and efficiency. Why does the FEC not require the use of their transaction codes, and why might a committee choose not to use them? They are essential for streamlining the reporting process for the **22,676** committees that report to the FEC by providing a structured system for recording, categorizing, and managing financial data. Then the FEC wouldn't have a reason to hide over 500 million uncategorized transactions from the public.

C. High Frequency Transactions and MTBD's

Data from SmurfSearch revealed **449,329,799** transactions where individuals donated to or through ActBlue. Here is a small sample of suspected high-frequency Smurfs, each contributing solely to ActBlue with a code 15 (Contribution to political committees [other than Super PACs and Hybrid PACs] from an individual, partnership or limited liability company). As mentioned earlier, 94% of donations ActBlue codes as 15's are attributed to these suspected Smurfs, totaling **$40,321,499**. To clarify, when ActBlue assigns a transaction code 15 (when they do assign codes), it usually means that's a donation specifically intended to go to them. Keep in mind that this does not include all the uncoded donations that have "Contribution to ActBlue" in the memo text. It would take a forensic audit to capture all of those.

Name	Total $ to ActBlue	Total FEC Ind NTRX	Trx to ActBlue Only (Code 15)	Total trx % to ActBlue
IMMASCHE, SONIA	$12,018.00	88,022	26,863	31%
KESKITALO, CANDACE	$18,319.00	66,837	12,312	18%
PUSCHECK, ROBERT	$16,219.00	50,104	16,163	32%
URBANOWICZ, WENDY	$17,169.00	55,701	14,429	26%
WESTERLUND, T	$9,133.00	42,032	15,621	37%
FIELDER, BETTY	$14,681.00	43,532	10,598	24%
DUMOND, DON	$1,718.00	49,035	1,588	3%
MASON, GWYN	$11,721.00	43,011	8,517	20%

Unusually high-frequency donating is one trait that characterizes a potential Smurf. Another indicator is identifying those with exceptionally high maximum transactions per day (MaxTBD), which refers to the maximum number of MSD Counts (multi-same-day transaction count) occurring within a single day within a committee ID for a particular contributor. See USB Stick "ActBlue Smurfs by MTBD" that includes only the top 125 out of **281,000** suspected unique Smurf names identified as contributing to and through ActBlue. The data is ranked from the highest to the lowest "Max TBD" donors. This figure is part of the donation profile of an unusually high-frequency donor known as a Smurf.

Also, see the USB stick titled "ActBlue Top MTBD," which contains the top 500 unique ActBlue donors who have contributed to and through ActBlue. The table below shows the top twenty names from that list, along with their unusually high MTBD figures. The term “Days with 25+ Trx” indicates how many days a donor had 25 or more transactions in a single day. This kind of irregular activity should trigger a fraud alert in merchant services if they are direct donations. If a donor uses the “Split-It” feature on the ActBlue website, click on the button to finalize the contributions, and their credit card will be charged for the full amount you authorized. The "Split It!" feature allows a donor to divide a single contribution amount equally among several political committees, with the total deducted from their card in one transaction.

CMTE ID	Name	MAX TBD	NUM TRX	AVG AMT$	Days with 25+ Trx
C00401224 - ACTBLUE	STOUT, E	4,437	19,007	$4.23	233
C00401224 - ACTBLUE	IMMASCHE, SONIA	2,589	65,272	$3.74	955
C00401224 - ACTBLUE	CAFFREY, DORO	2,350	5,359	$8.96	78
C00401224 - ACTBLUE	MUDE, AVINASH	2,267	8,155	$2.13	76
C00401224 - ACTBLUE	KIPPUR, SUSAN	2,078	5,105	$9.51	47
C00401224 - ACTBLUE	CONRAD, ROBERT	1,897	6,240	$13.83	66
C00401224 - ACTBLUE	ADAM, MONIQUE	1,812	16,908	$3.73	125
C00401224 - ACTBLUE	EVIDON, EVE	1,617	6,297	$6.18	115
C00401224 - ACTBLUE	ECKEL, RO	1,585	7,815	$2.05	117
C00401224 - ACTBLUE	PRAY, MERLE	1,582	17,591	$5.86	275
C00401224 - ACTBLUE	TEBRAKE, NORMA	1,540	4,018	$3.07	42
C00401224 - ACTBLUE	FUNK, CELIA	1,515	8,070	$10.31	128
C00401224 - ACTBLUE	OMARA, FRANCIS	1,465	3,078	$0.00	25
C00401224 - ACTBLUE	CHO, DR. JUN	1,439	9,866	$0.41	110
C00401224 - ACTBLUE	ALVES, DIANE	1,368	3,734	$9.79	47
C00401224 - ACTBLUE	BALES, DORLAN	1,345	16,502	$4.59	283
C00401224 - ACTBLUE	LEBON, RACHEL	1,336	2,985	$1.98	53

C00401224 - ACTBLUE	MACCLUER, JEAN	1,279	5,719	$2.39	92
C00401224 - ACTBLUE	GODBOLD, GARY	1,245	7,938	$20.31	73
C00401224 - ACTBLUE	QUINN, JIM	1,196	3,724	$0.76	31

The FEC NTRX data will not match the total NTRX shown by SmurfSearch. This is because the FEC historical data is constantly changing. Historical data should never change to ensure accountability and transparency. A federal agency destroying, altering, or falsifying historical data is a federal crime.

D. A/K/A names

A common tactic used by bad actors executing their Smurfing schemes is to employ various derivative spellings of real persons' names. The highest number of A/K/A names linked to a single individual in SmurfSearch is 91. For example, this person in Minnesota has 16 different versions of her name. If someone searches the FEC website using only the name at the top of this list, they will miss all the other contributions made under the different names shown here.

STROM, ROSE
aka: STROM, ROSE M
aka: STROM, ROSE M.
aka:STROM, ROSE MARY
aka:STROM, ROSE MARY MRS DONALD
aka:STROM, ROSE MARY MRSDONALD
aka:STROM, ROSE-MARY
aka:STROM, ROSE-MARY A
aka:STROM, ROSE-MARY DONALD
aka:STROM, ROSE-MARY MARY OTHER
aka:STROM, ROSE-MARY MRS
aka:STROM, ROSE-MARY MS.
aka:STROM, ROSE-MARY OTHER
aka:STROM, ROSE-MARY STROM
aka:STROM, ROSE-MARY(MRS
aka:STROM, ROSE-MARY(MRS.DONALD
aka:STROM, ROSE-ST.
aka:STROM, ROSEMARY
aka:STROM, ROSEMARY A.

E. Featured ActBlue Smurfs

The patterns described above exceed human capacity for manual donations and indicate smurfing techniques. SmurfSearch has identified **281,434** potential ActBlue Unique Smurfs. Only four are featured here. Like hundreds of thousands of Smurfs, all show high contribution transactions at the state and federal levels.

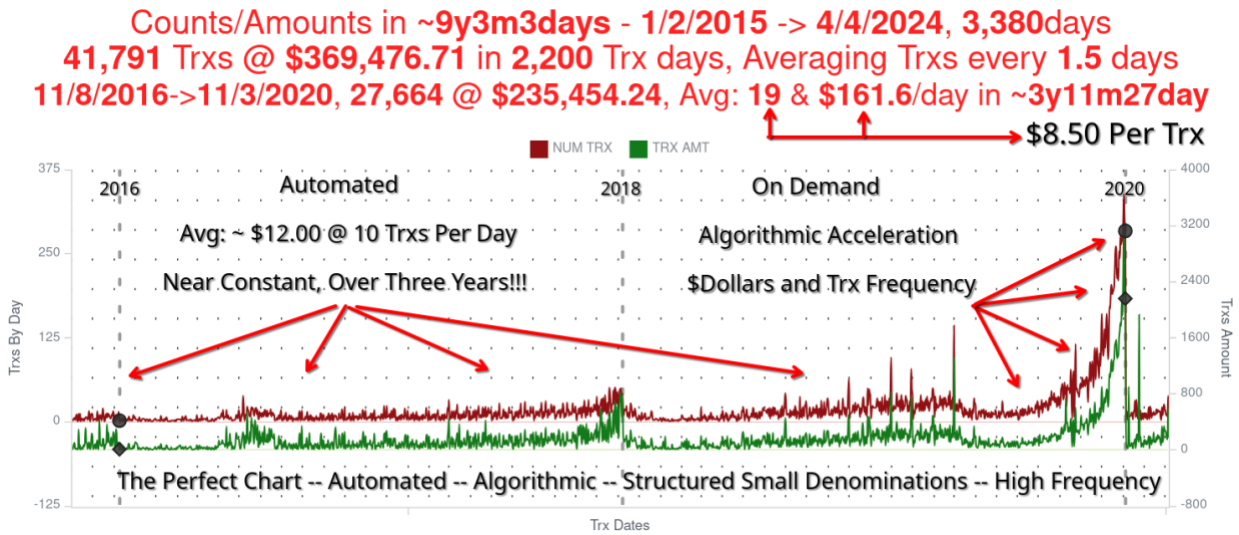
Steven Pilder, Pennsylvania

Over the past ten years, Mr. Pilder reports 41,791 direct and earmarked transactions to or through 119 federal committees, totaling $441,629.80 under zip code 19078; and an additional 2,038 direct and earmarked transactions to or through 9 federal committees, totaling $12,128.75 under zip code 19140. Both are the same person, as confirmed by his FEC statement, which indicates he is an ASSOCIATE PROFESSOR employed at TEMPLE UNIVERSITY SCHOOL OF MEDICINE.

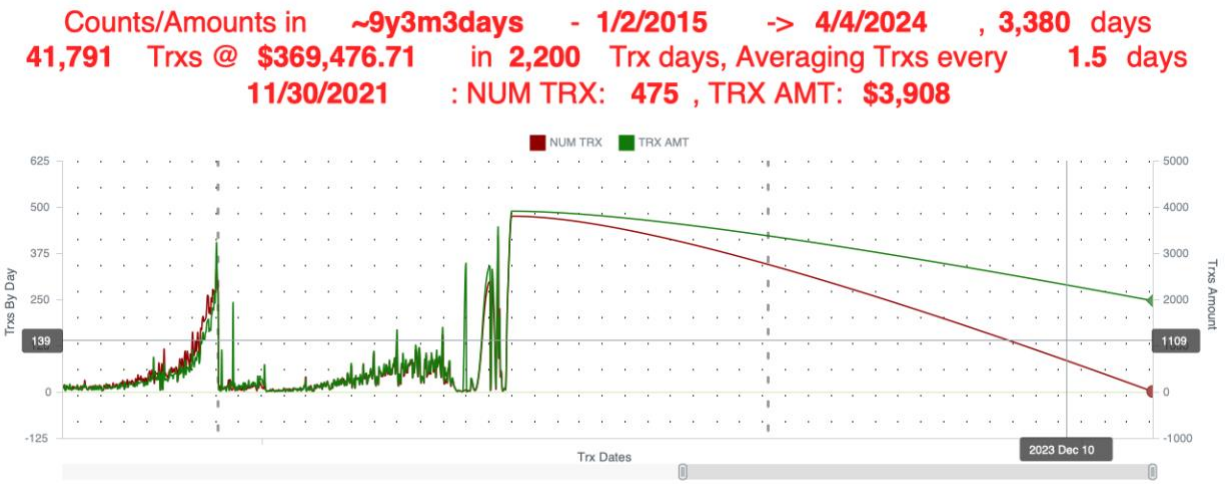
Transactions are recorded under two different zip codes in the same city and state, with the following aka's:

PILDER, STEPHEN
aka: PILDER, STEPHEN H
aka: PILDER, STEPHEN MS.
aka:PILDER, STEPHEN OTHER
aka:PILDER, STEPHEN,,,

This SmurfSearch interactive chart shows the daily number of contributions to all committees (red line), including those to and through ActBlue, and the corresponding dollar amounts (green line) for Mr. Pilder's zip code 19078. It illustrates all facets of Smurfing, such as automated donations versus the throttling of counts and amounts as elections approach.

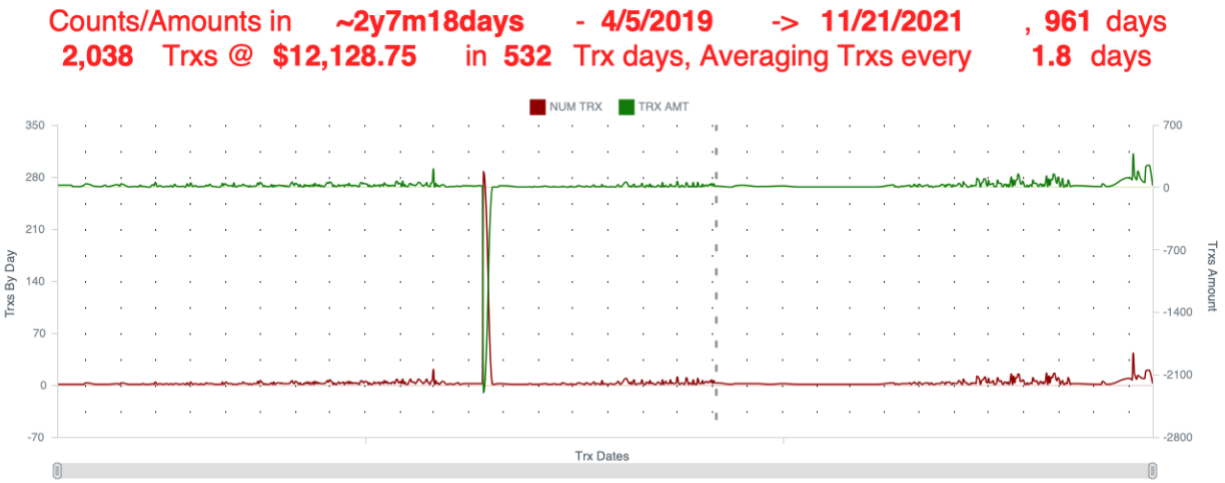


As shown in the next chart, Mr. Pilder's donations abruptly ceased on 10/6/2021, as reflected on his FEC statement as of 8/22/2025, which differs from what SmurfSearch recorded based on data from the Amazon S3 bucket (a cloud storage for the FEC database backup), showing 11/30/2021 with 475 NumTrxs totaling $3,908.00. Additionally, there was one more donation on 4/4/2024 for $1,971 using zip code 19078.



This chart below shows transactions attributed to Stephen Pilder from zip code 19140, with donations recorded between 4/5/2019 and 11/21/2021. Notably, on 4/13/2020, there were 287 transactions totaling -$2,300, marked "* REDESIGNATION TO WARREN DEMOCRATS, INC." in the memo text.

It is not illegal to donate from two different ZIP codes as long as the individuals are linked to those addresses and their contribution(s) are made with personal funds.



SmurfSearch breaks down transactions by committee for each donor, shown as "Num Trx." Here are the top 10 recipient committees out of 119 Mr. Pilder contributed to, highlighting the high volume of unusual transactions. The table also displays the Maximum Transaction by Day (labeled as "MAX TBD") for each committee, indicating the highest number of transactions on a single day for that specific committee.

CMTE ID	UID	NUM TRX	TOT AMT$	MAX TBD
C00401224 - ACTBLUE	PILDER, STEPHEN	25,044	$209,884.17	420
C00696526 - MARK KELLY FOR SENATE	PILDER, STEPHEN	2,142	$21,750.00	92

C00000935 - DCCC	PILDER, STEPHEN	1,550	$14,248.00	34
C00580068 - PROGRESSIVE TURNOUT PROJECT	PILDER, STEPHEN	1,056	$9,821.00	264
C00573261 - END CITIZENS UNITED	PILDER, STEPHEN	679	$4,773.00	5
C00508804 - SINEMA FOR ARIZONA	PILDER, STEPHEN	655	$8,283.00	16
C00716720 - HICKENLOOPER FOR COLORADO	PILDER, STEPHEN	631	$4,656.00	15
C00431056 - BOB CASEY FOR SENATE INC	PILDER, STEPHEN	586	$9,275.00	6
C00703975 - HARRIS FOR PRESIDENT	PILDER, STEPHEN	531	$4,503.00	8
C00633404 - STOP REPUBLICANS	PILDER, STEPHEN	524	$4,757.00	211

As shown above, Mr. Pilder has made 25,044 contributions to and through ActBlue from zip code 19078. SmurfSearch provides a breakdown of transaction codes attributed to each committee under his name. Here are the codes ActBlue reported to the FEC that went solely to and through ActBlue.

Trx Type	NUM TRX	TOT AMT$	MAX AMT$	AVG AMT$	MAX TBD	MAX ABD$
24T	17,284	$154,715.00	$300.00	$8.95	420	$3,554.00
	7,758	$55,149.17	$50.00	$7.11	36	$400.20
22Y	2	$20.00	$10.00	$10.00	2	$20.00
	Total 25,044	**Total $209,884.17**				

Most notable are the 7,758 uncoded transactions, which, upon further inspection of his FEC statement, are small donations to ActBlue and earmarked donations through ActBlue between 2015 and 9/2021.

Here are Mr Pilder's MTBDs (number of transactions across the SmurfSearch database on a single day) for the top 30 days. SmurfSearch data shows there are 1,074 days where transactions were recorded 10 times or more in a single day, indicating these donations are likely bot-generated.

Trx Date	Num Trx This Day	Tot Trx Amt$ This Day
10/19/20	233	$1,499.50
10/20/20	261	$1,532.83
10/21/20	258	$1,570.50
10/22/20	213	$1,306.50
10/23/20	227	$1,366.50
10/25/20	254	$1,597.50
10/26/20	243	$1,697.92

10/27/20	277	$1,815.43
10/28/20	264	$1,769.75
10/29/20	273	$2,155.00
10/30/20	269	$1,917.67
10/31/20	298	$2,541.00
11/1/20	339	$3,230.50
11/2/20	300	$2,233.25
11/3/20	284	$2,159.50
11/1/21	298	$2,715.00
11/4/21	282	$2,648.00
11/12/21	421	$3,564.00
11/14/21	224	$1,627.00
11/30/21	475	$3,908.00

Sonia Immasche, Colorado

Over the last ten years, Ms. Immasche reports 88,022 direct and earmarked transactions to or through 179 federal committees, totaling $441,629.80. The FEC NTRX data will not match the total NTRX shown by SmurfSearch. This is because the FEC historical data is constantly changing. Using the exact same filters on 8/20/25, the FEC shows 83,864 donations (or trx). Historical data should never change to ensure accountability and transparency. A federal agency destroying, altering, or falsifying historical data is a federal crime.

She has also contributed to candidates and committees in Wisconsin, Texas, and Michigan; 172, 49, and 200 times, respectively. Wisconsin Campaign Finance Information Systems show 172 contributions, of which 52 were listed as made through an ActBlue conduit. It is important to note that treasurers do not always report the conduit if a donation was received through one, so the total donations through ActBlue may be higher.

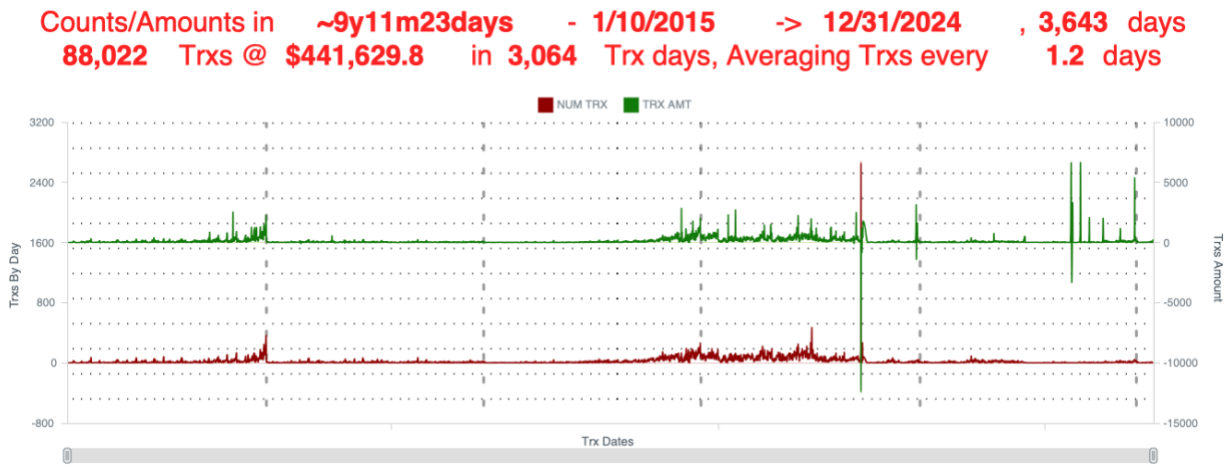
The first recorded date of retirement at the FEC is 1/28/2015.

Ms. Immasche, along with numerous other Smurfs interviewed in person and on video, has denied making the large amount of financial contributions attributed to her name.

Transactions are recorded under three different zip codes in the same city and state, with the following aka's:

IMMASCHE, SONIA
aka: IMMASCHE, SONIA IMMASCHE, SONIA, M,
aka: IMMASCHE, SONIA M
aka: IMMASCHE, SONIA M,
aka: IMMASCHE, SONIA M.
aka: IMMASCHE, SONIA MS.
aka: IMMASCHE, SONIA,

This SmurfSearch interactive chart shows the daily number of contributions to all committees (red line), including to and through ActBlue, and the corresponding dollar amounts (green line). The lines are mostly flat because of high-volume donations, with donations averaging every 1.2 days.



SmurfSearch breaks down transactions by committee for each donor, shown as "Num Trx." Here are the top 10 recipient committees out of 179 Ms. Immasche contributed to, highlighting the high volume of unusual transactions. The table also displays the Maximum Transaction by Day (labeled as "MAX TBD") for each committee, indicating the highest number of transactions on a single day for that specific committee. It's not humanly possible to make 2,589 transactions in one day, as shown to or through ActBlue. That would mean an average of 1.8 transactions per minute over that 24-hour period just to or through ActBlue.

CMTE ID	UID	NUM TRX	TOT AMT$	MAX TBD
C00401224 - ACTBLUE	IMMASCHE, SONIA	65,272	$244,063.01	2,589
C00580068 - PROGRESSIVE TURNOUT PROJECT	IMMASCHE, SONIA	934	$4,926.82	124
C00000935 - DCCC	IMMASCHE, SONIA	898	$9,120.00	13
C00748228 - MARCH ON PAC	IMMASCHE, SONIA	811	$4,320.00	25
C00745786 - DSI	IMMASCHE, SONIA	796	$2,767.50	101
C00659599 - PROGRESSIVE TAKEOVER	IMMASCHE, SONIA	762	$3,557.00	5
C00603084 - NDTC	IMMASCHE, SONIA	704	$3,558.00	7
C00562983 - DEMOCRATIC ACTION	IMMASCHE, SONIA	681	$6,109.00	7

C00633404 - STOP REPUBLICANS	IMMASCHE, SONIA	664	$3,417.50	112
C00718866 - JON OSSOFF FOR SENATE	IMMASCHE, SONIA	577	$4,531.60	52

As shown above, Ms. Immasche has made 65,272 contributions to and through ActBlue. SmurfSearch provides a breakdown of transaction codes attributed to each committee under her name. Here are the codes ActBlue reported to the FEC that went solely to and through ActBlue.

Trx Type	NUM TRX	TOT AMT$	MAX AMT$	AVG AMT$	MTBD	MAX ABD$
15	26,863	$12,018.00	$116.00	$0.45	117	$129.00
24T	22,342	$130,330.00	$3,300.00	$5.83	2,589	$3,300.00
	15,811	$101,429.01	$100.00	$6.42	64	$395.50
22Y	256	$286.00	$100.00	$1.12	107	$184.00
	Total 65,272	**Total $244,063.01**				

Analyzing the chart above shows that there are 15,811 transactions with no specified transaction type. Transaction code 15 indicates direct donations to ActBlue. However, there are actually more donations to ActBlue than shown here. By searching the FEC website and filtering out memos that say "contribution to ActBlue" without a transaction code, there are an additional 1,080 transactions. This means that 1,080 of the 15,811 transactions without a specified transaction type are donations to ActBlue.

Looking at the next highest committee Ms. Immasche donated to, the Progressive Turnout Project, there are 87 uncoded transactions. An actual real-time FEC search reveals "* EARMARKED CONTRIBUTION: SEE BELOW" populates all the memo texts, including those recorded as 15E.

Trx Type	NUM TRX	TOT AMT$	MAX AMT$	MIN AMT$	AVG AMT$	MAX TBD
	87	$414.82	$15.00	$1.00	$4.77	6
15E	722	$3,997.00	$300.00	$1.00	$5.54	6
22Y	125	$515.00	$15.00	$1.00	$4.12	124
	Total 934	**Total $4,926.82**				

Here are Ms. Immasche's MTBDs (number of transactions across the SmurfSearch database on a single day) for the top 30 days. SmurfSearch data shows there are 1,693 days where she donated more than 10 times in a single day, indicating these donations are likely bot-generated. Notably, there are 2,643 NumTrx totaling ($12,307.00) on 4/25/2022. Upon further investigation, it was found that these transactions no longer appear on the FEC website. However, there are

transactions on 4/30/22 involving 101 transactions with “INSUFFICIENT FUNDS” noted in the Memo_txt, with a load date of 5/12/2022 3:41:48 AM

Trx Date	Num Trx This Day	Tot Trx Amt$ This Day
4/30/22	268	$1,205.50
4/27/22	236	$1,192.00
4/25/22	2,643	($12,307.00)
11/15/21	177	$557.50
11/11/21	470	$388.00
11/10/21	277	$528.00
11/9/21	199	$1,972.00
11/7/21	271	$1,202.00
10/25/21	224	$427.00
10/10/21	190	$822.56
9/27/21	184	$785.29
9/26/21	251	$2,239.00
9/25/21	189	$759.00
9/22/21	206	$1,272.00
6/30/21	192	$806.00
5/30/21	223	$950.00
5/29/21	180	$624.00
12/31/20	179	$1,116.73
12/11/20	191	$622.00
11/2/20	264	$2,019.50
10/31/20	214	$1,363.00
10/29/20	185	$939.50
10/26/20	198	$1,207.00
10/6/20	187	$1,000.00
9/16/20	193	$817.00
11/7/16	363	$2,271.66
11/6/16	302	$1,633.00
10/31/16	247	$1,494.00
10/30/16	178	$1,223.00
10/19/16	179	$1,305.34

Mark Jennerjohn, Wisconsin

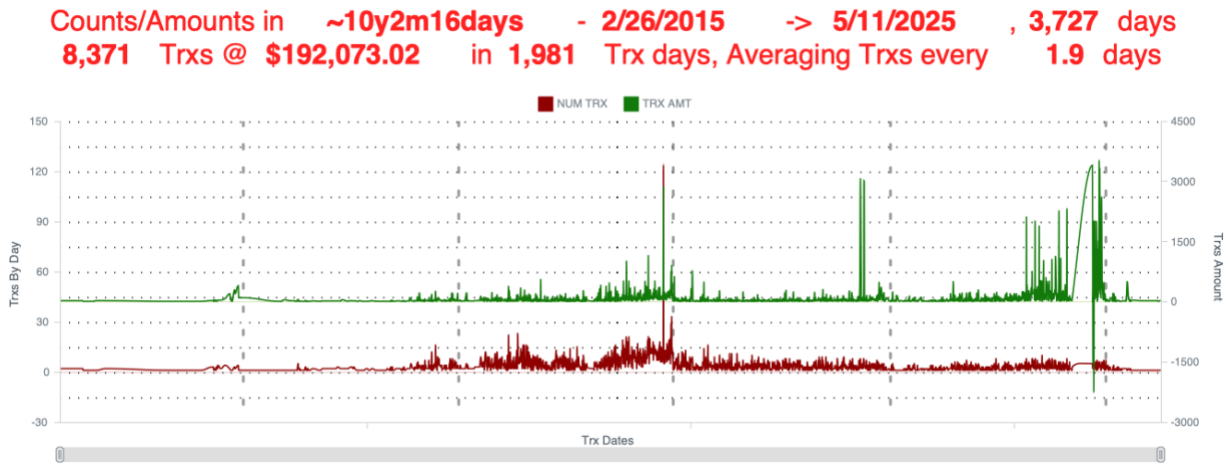
Over the past ten years, Mr. Jennerjohn reports 8,371 direct and earmarked transactions to or through 31 federal committees, totaling $192,073. He has also contributed to candidates and committees in Wisconsin, Texas, and Michigan: 172, 49, and 200 times, respectively. Wisconsin Campaign Finance Information Systems show 172 contributions, 52 of which were made through ActBlue as a conduit. It is important to note that reports indicate treasurers do not always list the conduit if a donation was received through one, so the total donations through ActBlue may be higher.

The first FEC recorded date of retirement is 10/01/2016.

Mr. Jennerjohn, along with many other Smurfs interviewed in person and on video, has denied making the large financial contributions attributed to his name. Here is a Rumble video showing the modest home where he lives, denying the contributions explained to him. Rumble: https://rumble.com/v4qk7si-the-silent-victims-elderly-citizens-and-political-corruption.html

Transactions are recorded under two different zip codes in the same city and state.

This SmurfSearch interactive chart shows the daily number of contributions to all committees (red line), including to and through ActBlue, and the corresponding dollar amounts (green line).



SmurfSearch breaks down transactions by committee for each donor, shown as "Num Trx." Here are the top 10 recipient committees out of 31 Mr. Jennerjohn contributed to, highlighting the high volume of unusual transactions. The table also displays the Maximum Transaction by Day (labeled as "MAX TBD") for each committee he gave to, indicating the highest number of transactions on a single day for that specific committee.

CMTE ID	UID	NUM TRX	TOT AMT$	MAX TBD
C00401224 - ACTBLUE	JENNERJOHN, MARK	5,638	$117,579.10	63
C00703975 - HARRIS FOR PRESIDENT	JENNERJOHN, MARK	507	$13,207.00	57

C00019331 - DEMOCRATIC PARTY OF WISCONSIN FEDERAL	JENNERJOHN, MARK	490	$8,735.00	4
C00492140 - AMERICAN BRIDGE 21ST CENTURY	JENNERJOHN, MARK	363	$11,852.00	7
C00010603 - DNC SERVICES CORP./DEM. NAT'L COMMITTEE	JENNERJOHN, MARK	338	$4,388.00	10
C00042366 - DSCC	JENNERJOHN, MARK	136	$1,226.00	3
C00746073 - MEIDASTOUCH LLC	JENNERJOHN, MARK	102	$1,024.00	2
C00484642 - SMP	JENNERJOHN, MARK	83	$1,777.00	3
C00614115 - NELSON FOR WISCONSIN	JENNERJOHN, MARK	81	$1,745.00	2
C00495028 - HOUSE MAJORITY PAC	JENNERJOHN, MARK	79	$2,356.00	2

As indicated above, Mr. Jennerjohn has 5,638 contributions to and through ActBlue. SmurfSearch then provides a breakdown of transaction codes attributed to each committee under his name. Here are the codes ActBlue reported to the FEC that went to and through ActBlue alone.

Trx Type	NUM TRX	TOT AMT$	MAX AMT$	AVG AMT$	MAX TBD	MAX ABD$
24T	3,893	$83,373.00	$1,500.00	$21.42	60	$2,000.00
	1,743	$34,204.10	$1,000.00	$19.62	11	$1,000.00
22Y	2	$2.00	$1.00	$1.00	2	$2.00
	Total 5,638	**Total $117,579.10**				

Analyzing the above chart shows that there are 1,743 transactions without a transaction type. There are no code 15's recorded like Ms. Immasche's. However, there are donations to ActBlue that are not shown here. By searching the FEC website and filtering out memos that say "contribution to ActBlue" without a transaction code, there are actually 150. This means that 105 of the 1,743 transactions without a transaction type are donations to ActBlue. The rest are direct and earmarked donations to committees.

Here are Mr Jennerjohn's MTBDs (number of transactions across the SmurfSearch database on a single day) for the top 30 days. SmurfSearch data shows there are 165 days where he donated more than 10 times in a day, indicating that these donations are likely bot-generated.

Trx Date	Num Trx This Day	Tot Trx Amt$ This Day
10/28/20	33	$900.00
10/26/20	29	$751.00
10/25/20	17	$270.70
10/23/20	20	$300.00
10/22/20	17	$282.00
10/19/20	19	$261.00
10/12/20	17	$208.00
9/30/20	123	$2,851.00

9/18/20	18	$361.00
8/26/20	18	$224.00
8/15/20	20	$300.00
8/12/20	16	$174.00
8/10/20	21	$1,143.00
8/8/20	19	$371.00
8/7/20	16	$128.00
7/5/20	17	$191.00
6/5/20	21	$514.00
6/1/20	18	$126.00
5/28/20	19	$1,004.00
5/27/20	21	$134.00
5/18/20	16	$516.00
5/15/20	19	$175.00
4/21/20	16	$370.00
6/25/19	16	$160.00
6/18/19	16	$292.00
6/13/19	16	$104.00
5/27/19	16	$176.00
5/26/19	23	$164.00
4/25/19	22	$384.00
8/21/18	16	$261.00

Ann Harrison, Texas

Over the past ten years, Ms. Harrison has made 31,725 direct and earmarked transactions to or through 111 federal committees, totaling $220,327.74. She has also donated to candidates and committees in Wisconsin 53 times, including 21 times to Governor Tony Evers during one election cycle. It is important to note that reports have indicated that treasurers do not always disclose the conduit if a donation was received through one.

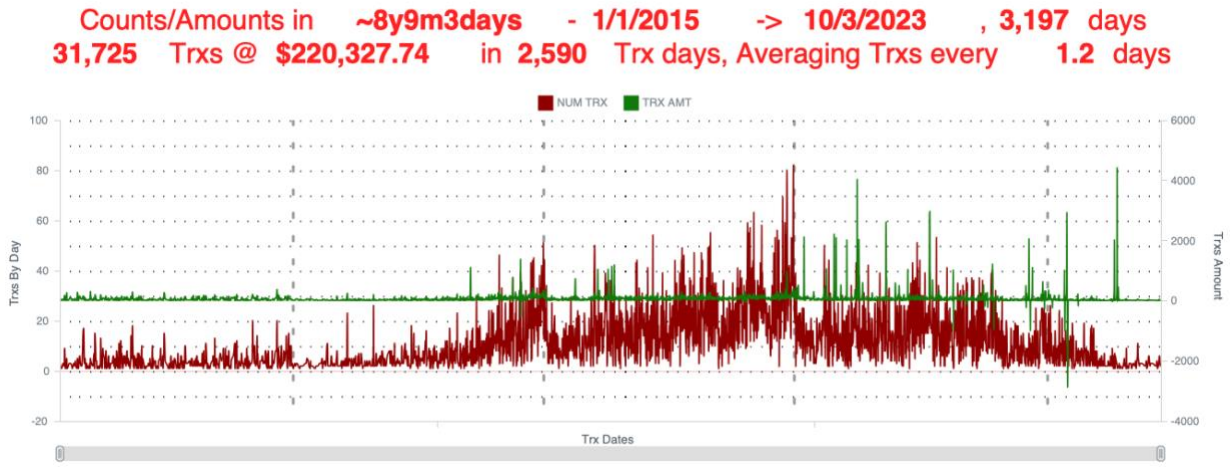
The first recorded date of retirement at the FEC is 1/1/2015.

Transactions are recorded under the following aka's:

HARRISON, ANN
aka: HARRISON, ANN ANN
aka: HARISON ANN M
aka: HARRISON, ANN MARIE
aka: HARRISON, ANN MARIE MARIE
aka: HARRISON, ANN MARIE MARIE MS.
aka: HARRISON, ANN MARIE OTHER

aka: HARRISON ANN MARIE,
aka: HARRISON, ANNMARIE

The SmurfSearch website displays the daily number of contributions to all committees, including to ActBlue (red line) and the corresponding dollar amount (green line) in these interactive charts.



SmurfSearch breaks down transactions by committee for each donor, shown as "Num Trx." Here are the top 10 recipient committees out of 111 Ms. Harrison contributed to, highlighting the high volume of unusual transactions. The table also displays the Maximum Transaction by Day (labeled as "MAX TBD") for each committee, indicating the highest number of transactions on a single day for that specific committee.

CMTE ID	UID	NUM TRX	TOT AMT$	MAX TBD
C00401224 - ACTBLUE	HARRISON, ANN	26,027	$151,769.72	62
C00573261 - END CITIZENS UNITED	HARRISON, ANN	455	$3,544.50	4
C00495028 - HOUSE MAJORITY PAC	HARRISON, ANN	363	$2,563.00	4
C00633404 - STOP REPUBLICANS	HARRISON, ANN	264	$1,375.00	3
C00580068 - PROGRESSIVE TURNOUT PROJECT	HARRISON, ANN	255	$2,190.00	4
C00632398 - LET AMERICA VOTE PAC	HARRISON, ANN	204	$1,236.00	5
C00000935 - DCCC	HARRISON, ANN	196	$2,770.00	4
C00603084 - NDTC	HARRISON, ANN	185	$1,855.00	2
C00748228 - MARCH ON PAC	HARRISON, ANN	171	$1,073.00	5
C00264697 - FRIENDS OF SHERROD BROWN	HARRISON, ANN	161	$1,249.00	4

As indicated above, Ms. Harrison has 26,027 contributions to and through ActBlue. SmurfSearch then provides a breakdown of transaction codes attributed to each committee under her name. Here are the codes ActBlue reported to the FEC that went to and through ActBlue alone.

Trx Type	NUM TRX	TOT AMT$	MAX AMT$	AVG AMT$	MAX TBD	MAX ABD$
15	10,878	$7,146.00	$270.00	$0.66	26	$278.00
	9,624	$69,126.72	$145.00	$7.18	38	$529.70
24T	5,516	$75,194.00	$2,900.00	$13.63	20	$4,008.00
22Y	9	$303.00	$270.00	$33.67	1	$270.00
	Total 26,027	**Total $151,769.72**				

The actual FEC export on 8/15/2025 for Ms. Harrison (using the same identifying information and filters, with her last recorded contribution on 10/3/2023) shows Trx Types (also known as transaction code types):

15's: all 10,878 "CONTRIBUTION TO ACT BLUE".
Uncoded: 10,106 (719 CONTRIBUTION TO ACT BLUE")
24T's: 5,083 all earmarked thru ActBlue.
22Y's: 0

There are at least three key insights: 1) how ActBlue's historical records of individual transactions consistently change at the FEC, which many researchers have long established. 2) upon further inspection, two different addresses are used for Ms. Harrison ([redacted]00 JACKSON AVE APT 2002 and [redacted]54 Far West Blvd Apt 2002), with the same apartment number and zip code, and contributions made on the same day hundreds of times. There exists a mix of coded and uncoded transactions. A credit card cannot have two different street addresses with the same zip code and apartment number registered at the billing address.

Here are Ms. Harrison's MTBDs (number of transactions across the SmurfSearch database on a single day) for the top 30 days. SmurfSearch data shows that there are 1,253 days on which she donated more than 10 times in a single day, indicating that these donations are likely bot-generated.

Trx Date	Num Trx This Day	Tot Trx Amt$ This Day
12/20/21	53	$205.00
10/25/21	51	$206.00
1/29/21	50	$182.00
10/31/20	82	$410.80
10/30/20	67	$361.00
10/27/20	48	$174.00
10/26/20	53	$288.00

10/25/20	53	$221.00
10/13/20	66	$227.00
10/12/20	80	$977.37
10/11/20	55	$227.50
10/10/20	54	$204.80
10/6/20	59	$254.00
9/30/20	69	$213.22
9/19/20	52	$233.80
9/14/20	56	$312.00
9/8/20	53	$227.00
7/31/20	58	$211.91
7/8/20	63	$242.50
6/27/20	57	$211.00
6/24/20	55	$214.50
6/20/20	59	$178.17
3/4/20	55	$279.00
2/29/20	49	$266.12
2/26/20	49	$177.00
1/17/20	47	$227.00
12/13/19	49	$193.00
9/19/19	54	$283.50
4/3/19	50	$266.50
11/5/18	51	$350.50

F. 462,147 Invalid Zip codes (See "Informational Notes and Terms" for further details)

The **281,434** unique ActBlue contributors in question, occurring from **2015-01-01** to **2024-12-31** [**~10 years 2 days**] collectively represent data from **74** different states (See USB stick "ActBlue States". Of these, there are **462,147** transactions with indeterminate ZIP codes. This count excludes cases where the city or state of a transaction matches or does not match its listed ZIP code. When invalid ZIP codes are identified, it remains impossible to verify whether the listed city or state is correct. Why doesn't ActBlue's current software include a feature to automatically verify or determine ZIP codes based on address information? Or does it have such a feature that is simply being ignored? When analyzing fraudulent transactions, "bad" or incorrect ZIP codes should raise red flags for several reasons. According to Google AI:

- **Bypassing Address Verification Systems (AVS):** Many online and offline payment systems use AVS to verify the billing address, including the ZIP code, provided by the customer against the information on file with the credit card issuer. If the ZIP code doesn't match, it can trigger a flag, which may indicate a

stolen card is being used. Fraudsters often use incorrect ZIP codes or mismatched ZIP codes with street addresses (e.g., a legitimate ZIP code but a fake address within it) to try and bypass these systems and complete purchases with stolen credit cards.

- **Evading Detection and Tracking:** Invalid addresses, including those with incorrect ZIP codes, are used to make it more difficult for businesses and law enforcement to track fraudulent activities back to the source. If a fraudster uses a non-existent or random address for a delivery, it makes it harder to trace the delivery back to them. This can include using fake addresses to redirect mail or packages and intercept them before the rightful recipient receives them.
- **Exploiting System Weaknesses and Avoiding Chargebacks:** Fraudsters might exploit vulnerabilities in address verification systems or use incomplete addresses (e.g., missing apartment numbers) to delay or complicate deliveries, which can make it easier to exploit return policies or make it harder for merchants to initiate chargebacks. By manipulating shipping labels or account addresses, they can redirect deliveries and try to receive refunds without returning the goods.
- **Circumventing Geographic Restrictions:** Fraudsters might provide an incorrect country or state on a form to access services or pricing that are geographically restricted. For instance, they might claim to be located in the United States to unlock shipping options or promotions only available to US customers, even if they're located elsewhere.

Inaccurate ZIP codes are often a telltale sign that someone is trying to bypass security measures, exploit loopholes, and ultimately commit fraud.

G ActBlue's Contributions and Many Names

The FEC website states that contributions from Political Action Committees (PACs) must be itemized on Schedule A, regardless of the contribution amount. The total value of ActBlue transactions is $12,075,259,87. ActBlue (FEC ID Committee number C00401224) reported only $4,847,225 in contributions to 364 committees and organizations on Schedule A since January 1, 2015, using 81 different name variations originating from the same address at ActBlue Headquarters in Somerville, MA 02144. As mentioned above, nearly $6 billion is coded as 24T treasury out, and another $6 billion in uncoded transactions, which include ActBlue direct donations to them, earmarked donations, and, to a lesser extent, various other obscure transactions. There is no way for the public to analyze whether there is a balance between incoming donations and if the donations went to the intended recipients. It would take a forensic

audit to investigate ActBlue's financial records and determine where the funds went, if they are recorded properly, and if the public is afforded all FEC records.

The table below lists the 81 different versions of the name "ActBlue" used for distributing $4,847,225.

ACTBLUE	aka:ACTBLUE, JIM
aka: ACTBLUE PAC	aka:ACTBLUE, JOANNE
aka: ACTBLUE (FEC ID C00401224)	aka:ACTBLUE, JOHN
aka:ACTBLUE AK-SEN 2026 DEMOCRATIC NOMINEE FUND CA-20	aka:ACTBLUE, LANA
aka:ACTBLUE C00401224	aka:ACTBLUE, LEAH
aka:ACTBLUE CALIFORNIA	aka:ACTBLUE, LESLIE
aka:ACTBLUE CIVICS, INC.	aka:ACTBLUE, LILA
aka:ACTBLUE FEDERAL OPERATING ACCOUNT	aka:ACTBLUE, LINDA
aka:ACTBLUE INC	aka:ACTBLUE, LISA
aka:ACTBLUE LLC	aka:ACTBLUE, LLC
aka:ACTBLUE NOMINEE FUNDS	aka:ACTBLUE, LUCIE
aka:ACTBLUE OF CALIFORNIA	aka:ACTBLUE, MARJORIE
aka:ACTBLUE PAC	aka:ACTBLUE, MARK
aka:ACTBLUE PAC.	aka:ACTBLUE, MARLEE
aka:ACTBLUE PACE	aka:ACTBLUE, MAX
aka:ACTBLUE TECHNICAL SERVICES	aka:ACTBLUE, MICHAEL
aka:ACTBLUE TECHNICAL SERVICES LLC, ACTBLUE TECHNICAL SE	aka:ACTBLUE, MITCHELL
aka:ACTBLUE, ,	aka:ACTBLUE, NANCY
aka:ACTBLUE, ACTBLUE	aka:ACTBLUE, NINA
aka:ACTBLUE, ADAM	aka:ACTBLUE, NORMA
aka:ACTBLUE, AHMAD	aka:ACTBLUE, PAC
aka:ACTBLUE, ALI	aka:ACTBLUE, PATRICIA
aka:ACTBLUE, AMY	aka:ACTBLUE, PETER
aka:ACTBLUE, BARRY	aka:ACTBLUE, PRISCILLA
aka:ACTBLUE, BETH	aka:ACTBLUE, RD
aka:ACTBLUE, BETSY	aka:ACTBLUE, REGINALD
aka:ACTBLUE, BETTY	aka:ACTBLUE, RITA
aka:ACTBLUE, BRIAN	aka:ACTBLUE, ROBERT
aka:ACTBLUE, CAROL	aka:ACTBLUE, SANDY
aka:ACTBLUE, CAROLYN	aka:ACTBLUE, SERVICES
aka:ACTBLUE, DANIALLE	aka:ACTBLUE, STANFORD
aka:ACTBLUE, DAVID	aka:ACTBLUE, STEPHEN
aka:ACTBLUE, DENISE	aka:ACTBLUE, SUE ELLEN
aka:ACTBLUE, DIANE	aka:ACTBLUE, TIMOTHY
aka:ACTBLUE, ELIZABETH	aka:ACTBLUE, VERNON
aka:ACTBLUE, ELLEN	aka:ACTBLUE, WENDY
aka:ACTBLUE, ERICA	aka:ACTBLUE, WRIGHT
aka:ACTBLUE, FED (AMALG	aka:ACTBLUE, ZINA
aka:ACTBLUE, JANE	aka:ACTBLUEP AC

	aka:ACTBLUEPAC

Notably, multiple organizations use the same committee number. For example, ActBlue Civics, a branch of ActBlue that helps left/liberal 501(c)(4)s build grassroots movements with online fundraising tools, is an issue advocacy group filed with the IRS as a 501(c)(4). They are legally separate entities with distinct registrations and should not share a committee number. The same applies to ActBlue Technical Services, a different nonprofit organization that provides engineering and infrastructure support for the broader ActBlue network. As a technical service provider rather than a political committee that raises and spends federal funds, it has its own legal identity and should not use the FEC number of the ActBlue PAC when making donations. Additionally, ActBlue LLC listed above does not appear to exist.

See the USB Stick "**ActBlue Contributions"** which displays all 364 PACs and organizations that the above ActBlue entities contributed to.

A side note, Rebellion Pack (treasurer Cenk Uygur) https://www.fec.gov/data/committee/C00727008/?tab=about-committee&cycle=2022 received $921,135 directly from ActBlue. (A real-time FEC lookup of "Rebellion" PAC shows $894,881 between 11/21/2019 and 3/31/2020.) SmurfSearch indicates ActBlue classified 51 donations to the Rebellion PAC as Code 15 (contributions to political committees [other than Super PACs and Hybrid PACs] from individuals, partnerships, or LLCs). The Rebellion PAC is registered as a Hybrid PAC, but Code 15 excludes Hybrid PACs. Were these direct donations from ActBlue from a Hybrid PAC to a Hybrid PAC illegal? Or was it sloppy reporting? Furthermore, ActBlue is the fundraising platform for the Rebellion PAC https://secure.actblue.com/donate/rebellion-pac-1.

This table displays examples of the entities listed in order from the top MTBD's that ActBlue dispersed contributions to. The transaction codes include 5, 15E, 22Y, and blank uncoded.

CMTE ID	UID	NUM TRX	TOT AMT$	MAX TBD
C00853481 - DEMOCRATS WHO WIN	ACTBLUE	2,052	$73,916.00	860
C00042366 - DSCC	ACTBLUE	1,319	$95,221.00	244
C00659599 - PROGRESSIVE TAKEOVER	ACTBLUE	1,999	$51,436.00	224
C00580068 - PROGRESSIVE TURNOUT PROJECT	ACTBLUE	4,198	$100,047.00	116
C00847483 - SHAWN FOR GEORGIA	ACTBLUE	962	$183,697.00	108
C00837062 - ANDREI FOR ARIZONA	ACTBLUE	684	$305,477.00	98
C00633925 - JUSTICE 2018	ACTBLUE	155	$128,800.00	84
C00632398 - LET AMERICA VOTE PAC	ACTBLUE	503	$16,547.00	55
C00577130 - BERNIE 2016	ACTBLUE	99	$34,757.00	41
C00765800 - FETTERMAN FOR PA	ACTBLUE	97	$4,661.00	41
C00495580 - STABENOW VICTORY FUND	ACTBLUE	64	$165,350.00	41

More of this same type of activity is recorded under the address in Cambridge, MA from zip codes 02238, 02139, and 02138 to total $1,246,078. Seems there are ActBlue satellite addresses

listed in Cambridge, MA using zip code 02138 and 02238, but not 02139, using the different versions of ActBlue not listed as legal contributors under Committee C00401224.

More	ACTBLUE aka: ACTBLUE - CONDUIT FUNDRAISING COMMITTEE aka: ACTBLUE - CONDUIT FUNDRAISING COMMITTEEE aka:ACTBLUE PAC aka:ACTBLUE TECHNICAL SERVICES aka:ACTBLUE, ACTBLUE aka:ACTBLUE- CONDUIT FUNDRAISING COMMITTEE aka:ACTBLUE.

More	ACTBLUE aka: ACTBLUE CALIFORNIA aka: ACTBLUE TECHNICAL SERVICES aka:ACTBLUE TECHNOLOGIES, INC. aka:ACTBLUE/AUBURN QUAD, INC.

Below are summaries of eight different ActBlue versions where ActBlue recorded contributions to the FEC under various names, many of which involve large dollar amounts. See USB stick "ActBlue Many Names" to view all contributor data per version.

NAME -> Starts with 'ACT BLUE'
7 Contributors: 850 Transactions - Total: $258,122.00
MaxAmt: $26,723.00 , MinAmt: $-250.00 , MaxTBD: 34 , MaxABD: $26,723.00

NAME -> Starts with 'BLUE, ACT'
8 Contributors: 111 Transactions - Total: $46,416.52
MaxAmt: $5,000.00 , MinAmt: $-100.00 , MaxTBD: 7 , MaxABD: $5,000.00

NAME -> Starts with 'ACT, BLUE'
60 Contributors: 732 Transactions - Total: $19,644.79
MaxAmt: $1,250.00 , MinAmt: $1.00 , MaxTBD: 167 , MaxABD: $1,571.57

NAME -> Contains 'ACCTBLUE'
1 Contributors: 1 Transactions - Total: $1,000.00
MaxAmt: $1,000.00 , MinAmt: $1,000.00 , MaxTBD: 1 , MaxABD: $1,000.00

NAME -> Contains 'ACCTBLUE'
1 Contributors: 1 Transactions - Total: $1,000.00
MaxAmt: $1,000.00 , MinAmt: $1,000.00 , MaxTBD: 1 , MaxABD: $1,000.00

NAME -> Contains 'ACTBLUE PAC'
4 Contributors: 5 Transactions - Total: $485.00
MaxAmt: $250.00 , MinAmt: $25.00 , MaxTBD: 1 , MaxABD: $250.00

NAME -> Starts with 'ACTBLUE, ACTBLUE'
1 Contributors: 3 Transactions - Total: $53.62
MaxAmt: $27.00 , MinAmt: $2.42 , MaxTBD: 2 , MaxABD: $27.00

Lack of transparency makes transactions difficult to trace, which indicates deception. This is a red flag for potential criminal activity within this committee.

In conclusion, "ActBlue" is the only registered name at the FEC under Committee C00401224. It is illegal to use the name of another, stealing an identity, or create a new one to deposit funds. This is considered a federal crime, as they apparently did by using over 80 different name variations to make contributions. It would take a forensic audit to uncover the real source of these troubling, highly suspicious contributions that strongly resemble Smurf activity.

H. "Blue" Synthetic Identity Laundering to and through ActBlue

While reviewing different versions of ActBlue's names and the donations connected to them, a concerning pattern became clear. (See USB Stick: Blue in Name). There are 4,598 names that include "blue." Some may be legitimate names. These names not only contain "blue" but also seem linked to unusual names and their recorded entity types, which are likely used to hide rather than reveal the true source. There are a very unusual amount of "Blue" as a surname with the same last name from multiple zip codes. Collectively, this strongly suggests that an algorithm was used to deposit these funds. Keep in mind that these are just the "Blues," and they could go unnoticed because very few transactions are tied to each name, adding to the Smurf total in this complaint. A forensic audit is needed to identify all other irregular name patterns. Several warning signs of improper categorization and synthetic identity laundering include:

1) Bizarre names that include. Especially notable is "UNITEMIZED RECIEPTS, FROM ACTBLUE":

Name	City	State	Zip	Num Trx	Tot Amt$
BLUE EYES, THOMAS	OKLAHOMA CITY	OK	73139	5	$134.00
ACTBLUE NIJJAR, VIKRUM	NOVATO	CA	94949	2	$2,000.00
ACTBLUEKPORTER, KIMG	CHINO	CA	91710	1	$15.00
BLUE, **POPS	SMITHFIELD	RI	2917	2	$30.00
LOVEJOYBLUEM, ARLENE	BURBANK	CA	91510	2	$13.20
ST.JACQUESBLUE, DI	WINTER PARK	FL	32792	12	$462.00
WAT, SHAINA ACT BLUE	BROOKLYN	NY	11201	1	$10.00
UNITEMIZED RECIEPTS, FROM ACTBLUE	SOMERVILLE	MA	2144	7	$123,119.06
BLAH, BLUE	HURRICANE	WV	25526	2	$20.00

2) Same names from different locations that include foreign donations, which is a federal crime. Especially notable are the 77 total donations from Bluestone, Allan from two different addresses in London and Valentine, Blue from three different states.

Name	City	State	Zip	Num Trx	Tot Amt$
BLUE, BIG	HOESBACH	ZZ	63768	1	$50.00
BLUE, CHRISTIAN	OSTERFARNEBO	ZZ	811 9	1	$25.00
BLUE, LEON	NAHON PHANOM	ZZ	48000	1	$100.00
BLUE, LIAN	LONDON	ZZ	E17 6	1	$50.00
BLUESTONE, ALLAN	BRUSSELS 1180 BELGIUM	ZZ	0	153	$697.00
BLUESTONE, ALLAN	BRUSSELS MA 01180 BELGIUM	ZZ	0	24	$86.00
WEISS, BLUE	LONDON	ZZ	N88LD	65	$2,304.11
WEISS, BLUE	LONDON N88LD UNITED KINGDOM	ZZ	0	32	$1,260.00
WEISS, BLUE	LONDON N8 8LD UNITED KINGDOM	ZZ	0	7	$441.00
WEISS, BLUE	LONDON	ZZ	N8 8L	4	$151.00
VALENTINE, BLUE	ALBANY	OR	97321	17	$81.00
VALENTINE, BLUE	VALLEY VILLAGE	CA	91607	6	$15.00
VALENTINE, BLUE	SAN ANTONIO	TX	78218	2	$600.00

3) There are 1,100 unique names with “Blue” as a surname, with first names ranging from A to Z, excluding only the letter X (see USB Stick “Blue Surname”). These names come from multiple first names across different zip codes. This statistically suggests automated name generation and strongly indicates that these records are not from real human donors but are likely synthetic data created to appear diverse. They seem designed to avoid easily detectable duplication. Smurfsearch researchers note this common tactic used in most Smurfed committees.

4) There are 314 unique names (“Blue First Name”) with surnames from A to Z, excluding only the letters U, X, and Z. Some names are quite bizarre. This pattern suggests automated name generation and strongly indicates that these records are not from real human donors but instead are scripted identity fabrications. Here are a few examples:

MACELLARI, BLUE from 4 different zip codes
SKY, BLUE from 3 different zip codes
BONETTE, BLUEHOUSE
BOSTOCK, BLUE HAIR STUDIO
CROSSMAN, BLUEBIRD
CURTISS, BLUERAY
DEERWOMON, BLUESTAR
FAMILY, BLUE CROSS BLUE SHEI

BLAH, BLUE
GIBSON, BLUE RAINCOAT
HINMAN, BLUEBERRY HUFFLEPUFF

5) Same names appearing across multiple cities, states, or ZIP codes, like different versions of Robert Blue. Even if some of these are legitimate donations, it is still noteworthy.

Name	City	State	Zip	Num Trx	Tot Amt$
BLUE, ROBERT	KIRKLAND	WA	98033	3	$300.00
BLUE, ROBERT	RICHMOND	VA	23225	75	$171,423.00
BLUE, ROBERT	RICHMOND	VA	23219	125	$108,758.00
BLUE, ROBERT	RICHMOND	VA	23261	1	$3,500.00
BLUE, ROBERT	ABILENE	TX	79602	1	$21.07
BLUE, ROBERT	AUSTIN	TX	78737	4	$47.00
BLUE, ROBERT	FULSHEAR	TX	77441	2	$450.00
BLUE, ROBERT	HOUSTON	TX	77069	1	$200.00
BLUE, ROBERT	SAN ANTONIO	TX	78249	1	$5.00
BLUE, ROBERT	MURFREESBORO	TN	37127	2	$200.00
BLUE, ROBERT E. JR.	CEDARS	PA	19423	2	$1,250.00
BLUE, ROBERT WILDER	SCAPPOOSE	OR	97056	9	$73.50
BLUE, ROBERT	CLEVELAND	OH	44112	16	$147.00
BLUE, ROBERT	BUFFALO	NY	14206	26	$508.50
BLUE, ROBERT	BUFFALO	NY	14215	1	$10.00
BLUE, ROBERT	HARRISON	NY	10528	3	$45.00
BLUE, ROBERT	NEW YORK	NY	10014	10	$169.50
BLUE, ROBERT	GRAND ISLAND	NE	68801	7	$57.24
BLUE, ROBERTA	CHAPEL HILL	NC	27514	13	$422.00
BLUE, ROBERTA	WALKERTOWN	NC	27051	1	$25.00
BLUE, ROBERT	MANDEVILLE	LA	70471	2	$800.00
BLUE, ROBERT	SHREVEPORT	LA	71105	62	$4,078.92
BLUE, ROBERT L	DELPHI	IN	46923	1	$500.00
BLUE, ROBERT	CHICAGO	IL	60628	2	$20.00
BLUE, ROBERT	CHICAGO	IL	60614	1	$25.00
BLUE, ROBERT	TINLEY PARK	IL	60477	4	$71.00
BLUE, ROBERT	AUSTELL	GA	30168	14	$244.50
BLUE, ROBERT	ORLANDO	FL	32803	24	$819.86
BLUE, ROBERT	PANAMA CITY	FL	32401	2	$750.00
BLUE, ROBERT	DENVER	CO	80205	1	$10.00
ACTBLUE, ROBERT	CANOGA PARK	CA	91303	3	$60.00
BLUE, ROBERT	COMPTON	CA	90222	1	$25.00
BLUE, ROBERT	FAIR OAKS	CA	95628	1	$250.00
BLUE, ROBERT	NAPA	CA	94558	34	$10,129.50

BLUE, ROBERT	SAN CLEMENTE	CA	92672	1	$25.00
BLUE, ROBERT	SAN DIEGO	CA	92126	6	$99.50
BLUE, ROBERT WILDER	SAN FRANCISCO	CA	94117	24	$543.40
BLUE, ROBERT	UKIAH	CA	95482	35	$4,744.00
BLUE, ROBERT	SCOTTSDALE	AZ	85251	6	$775.00
BLUE, ROBERT	LITTLE ROCK	AR	72223	1	$300.00

6) 60 Act, Blue where Act is the surname and Blue is the first name, from 60 different zip codes. (see USB stick "Act Surname, Blue Last")

7) 26 versions that include "ActBlue" as a surname from 26 different zip codes. Especially notable is "SMALL DONORS ON ACTBLUE, SMALL DONORS" who donated twice to total $3,382.21

Name	City	State	Zip	Num Trx	Tot Amt$
ACTBLUE, ABIGAIL	NO SIR	VT	0	1	$10.00
ACTBLUE, DFA	BURLINGTON	VT	5401	23	$99.00
ACTBLUE, DEE	NEW YORK	NY	10014	1	$10.00
BURKE ACTBLUE, DAVID	NEW YORK	NY	10040	7	$52.50
ACTBLUE, KLARE	PLAINVIEW	NY	11803	1	$25.00
ACTBLUE, ANONYMOUS	SPRINGFIELD	PA	19064	1	$5.00
ACTBLUE, MATTEUS	MELBOURNE	FL	32935	2	$50.00
BALDOR ACTBLUE, CRISTINA	MIAMI	FL	33130	35	$875.00
ACTBLUE, ERICH	MIAMI	FL	33134	1	$25.00
GIOVANNIACTBLUE, CLAYTON	COLUMBUS	OH	43227	34	$1,315.00
ACTBLUE, ANTHONY	DEARBORN HEIGHTS	MI	48127	1	$27.00
BLAHUNKA-ACTBLUE, GARRETT-ACTBLUE	PAW PAW	MI	49079	3	$125.00
KURTENBACHACTBLUE, LAURA	KANSAS CITY	MO	64108	2	$19.80
ACTBLUE, R	PHOENIX	AZ	85032	19	$282.90
JACTBLUE, PAUL	SCOTTSDALE	AZ	85252	2	$22.00
SMALL DONORS ON ACTBLUE, SMALL DONORS	CONGRESS	AZ	85332	2	$3,382.21
ACTBLUE, ROBERT	CANOGA PARK	CA	91303	3	$60.00
ACTBLUE, GREG	ANAHEIM	CA	92801	2	$26.00
ROE C/O ACTBLUE, JO	BELMONT	CA	94002	6	$5,500.00
MCDOUGALLWEILACTBLUE, ALISON	SUNNYVALE	CA	94086	1	$100.00
ACTBLUE, ACTBLUE	BERKELEY	CA	94704	3	$53.62
KHALIMACTBLUE, EUGENE	STOCKTON	CA	95209	1	$1.00
ACTBLUE, QUAN	LYNNWOOD	WA	98087	1	$10.00
ACTBLUE, MELI	SEATTLE	WA	98104	192	$1,310.30
ACTBLUE, SARAH	SEATTLE	WA	98116	54	$52.00

ACTBLUE, SARAHTEST	SEATTLE	WA	T7Z1A	1	$1.00

III. VIOLATIONS ALLEGED

The conduct described in Section III gives rise to multiple violations of the Federal Election Campaign Act (FECA) and associated federal regulations. Each of the following violations is supported by the structured data, spreadsheet analysis, and third-party reporting referenced in the factual record.

Count I – Contributions in the Name of Another
Violated: 52 U.S.C. § 30122 and 11 C.F.R. § 110.4(b)
ActBlue accepted contributions that, on their face, were not from the true source. Donor names used thousands of times across multiple committees, in state and federal campaigns, indicate that a single or coordinated entity was contributing in the names of others. Additionally, the high maximum transaction counts per day per contributor in the SmurfSearch database, especially from high-frequency contributors, should raise red flags.

Whether through reimbursement schemes, identity fabrication, or credential pooling, this activity squarely violates FECA's ban on "contributions in the name of another."

Count II – Failure to Accurately Report the Purpose or Source of Contributions
Violated: 52 U.S.C. § 30104(b) and 11 C.F.R. § 104.3(b)
Per MUR 7923, the FEC has found that mislabeling or failing to account for the true purpose of disbursements or source of funds constitutes a material violation.
Campaign reports show:
-ActBlue did not accurately disclose the true source of at least 178,204,660 contributions.
-High-frequency accounts that log thousands of entries (e.g., SONIA IMMASCHE with over 88,000 transactions);
- Concealing donations by not applying transaction codes to 388,748,632 to hide the true source and/or intent of incoming funds.

Count III – Failure to Implement Internal Controls to Prevent Fraudulent Contributions
Violated: FECA compliance responsibilities; interpreted via prior MURs and Commission guidance. ActBlue accepted contributions without performing due diligence despite glaring anomalies in:
-Donor employment status,
-Indeterminate zip codes,
-Zip codes that do not match the City/State,
-Inconsistency in coding transactions,
-Inconsistent memo text verbiage,
-Lack of transaction codes,
-High volume of same day transactions per donor,
-Deviant name distributions,
-Uniform contribution amounts,
-Timestamp synchrony.

Under Commission expectations, a reasonable campaign must screen for laundering or identity misuse. The failure to do so—when data was plainly available in the campaign's own FEC filings—constitutes gross negligence or willful blindness.

Count IV – Failure to Maintain Contributor Records
Statute/Rule Violated: 52 U.S.C. § 30102(c)(5), 11 C.F.R. § 102.9(a)–(b)
Campaigns must retain full contributor records, including names, addresses, occupations, and employers, for any contributor whose aggregate total exceeds $200. Numerous contributions appear to be linked to synthetic or cloned donors—some of whom could not be real people or could not have contributed lawfully.
ActBlue lacked verifiable records for:
-High-volume donors like Sonia Immasche or Mark Jennerjohn,
-Elderly individuals whose family members later denied the donations,

Count V – Failing to Use Best Efforts to Obtain Contributor Information
Statute/Rule Violated: 52 U.S.C. § 30102(c)(2), 11 C.F.R. § 104.7(b)
FECA requires committees to exercise "best efforts" to obtain and report the full name, mailing address, occupation, and employer of each contributor.
-Many donor records:
-Lack valid employer information (e.g., widespread use of "not employed"),
-Contain generic or implausible addresses, or
-Were submitted with known unverifiable payment methods (e.g., via ActBlue without CVV).
ActBlue accepted funds from unverifiable sources and did not follow up to obtain correct identifying information, it violated the best-efforts standard.

Count VI – Knowingly Accepting Excessive Contributions from a Single Source Using Different Names
Even if each smurfed micro-donation was below the $3,300 per-election limit, accepting multiple contributions that were knowingly made by one source using different Smurfs (also referred to a straw donors) constitutes a single excessive contribution.

Count VII – Reporting Fraudulent Contributions as Lawful Contributions
Statute/Rule Violated: 52 U.S.C. § 30104(b)(3), 11 C.F.R. § 104.3(a)(4)
ActBlue reported smurfed contributions using names of individuals who did not give the money, or if contributions were entered automatically or with spoofed credentials, then each such filing constitutes a false report of a lawful contribution. This count reinforces Count II, but focuses specifically on fraudulent miscategorization of donations.

IV. REQUESTED ACTIONS

Based on the statutory violations, structured financial evidence, and public record analysis presented in this complaint, the Commission is urged to take the following actions. These are categorized below into civil enforcement actions under the Commission's authority, and criminal referrals appropriate under 52 U.S.C. § 30109(c) and 18 U.S.C. §§ 1001, 1343, and 1956.

A. Civil Enforcement – Requested FEC Actions

1 Find Reason to Believe that ActBlue and any responsible individuals violated provisions of FECA, all the cited statutes and rules above, including 52 U.S.C. §§ 30122, and 30104.

2 Open a Full Investigation, including the issuance of subpoenas for:
-Donation metadata from ActBlue (IP addresses, submission timestamps, CVV usage logs, financial transactions);
-Merchant processors such as Stripe, Gift-To-Gram, Divvy Cards (now Bill.com), Paypal, Democracy Engine, and others to be listed upon request or in future court filing;
-Internal compliance communications and donor vetting procedures.
-Forensic Audit each of ActBlue Committees' Records

3 Conduct a full audit of ActBlue's donation processing system, with special attention to: Contributions over $6,600 from single donors; all entries tied to "Not Employed," "Retired," "N/A", or "Unemployed" donors; repeated entries with identical timestamps and dollar amounts.

4 Impose Civil Penalties
Seek the maximum available monetary penalties under 52 U.S.C. § 30109(d) for:
Each excessive contribution received;
Each materially false or misreported entry;
Each willful failure to refund or report illegal contributions.

5 Order Public Correction of Reports Requiring ActBlue to:
-File amended FEC reports correcting all contributions falsely attributed, mischaracterized, or exceeding legal limits;
-Recalculate compliance totals for all donors affected;
-Refund all excessive or illegally attributed contributions.
-Mandate Implementation of Internal Controls
-Direct the campaign to adopt and certify a compliance protocol including:
-CVV requirement for all credit card donations;
-Mandate card verifications to the name of the person, to their physical address, to the name of their financial institution, to the physical address of the associated branch;
-Donor identity verification thresholds;
-Automatic flagging of high-volume microdonors and outlier contribution patterns.

B. Criminal Referral – Requested DOJ Actions
In accordance with 52 U.S.C. § 30109(c), Complainant requests that the FEC refer this matter to the U.S. Department of Justice for criminal investigation. The conduct described herein supports a reasonable inference that knowing and willful violations of federal law have occurred.
1 Refer the Matter to the U.S. Department of Justice – Public Integrity Section For criminal prosecution of:
-18 U.S.C. § 1001 – Filing false statements with a federal agency (false FEC contributor identities);
-18 U.S.C. § 1343 – Wire fraud (use of online systems to defraud the government and the public);
-18 U.S.C. § 1956 – Money laundering (structuring of donations to disguise the source of funds);

-18 U.S.C. § 2 – Aiding and abetting by campaign staff or third-party processors.

2 Investigate Potential Conspiracy
Investigate whether campaign personnel, fundraising vendors, data analysts, or other affiliated individuals or firms conspired to knowingly use software, lists of elderly identities, or alias donation schemes to structure contributions in violation of FECA.

3 Protect Elderly or Vulnerable Donors from Identity Misuse
Investigate whether any civil rights or elder protection laws were violated by the repeated listing of elderly or incapacitated individuals as donors without their knowledge or consent.

4 18 U.S.C. § 371 – Conspiracy to Commit Offense or to Defraud the United States
Why applicable: If two or more persons conspired to structure donations, falsify donor records, or evade FECA reporting requirements, this statute is implicated. Smurfing operations typically involve coordinated behavior among digital payment processors, fundraisers, and data handlers. Example application: Coordinated donor identity spoofing using ActBlue, joint donor laundering strategies by campaign staff and fundraising firms.

5. 18 U.S.C. § 1028 – Fraud and Related Activity in Connection with Identification Documents
Why applicable: This statute criminalizes knowingly producing or using false identification documents or information—including names, addresses, or employer info—to commit fraud. Example application: Use of fabricated or misappropriated donor names to break up large illegal contributions into smaller ones attributed to straw donors.

6. 18 U.S.C. § 1028A – Aggravated Identity Theft
Why applicable: If smurfing operations used actual, real people's identities without their permission (especially seniors), this provision adds a mandatory 2-year consecutive prison sentence. Example application: ActBlue's donor lists include elderly individuals who deny making donations—indicating their identities were used without authorization.

7. 18 U.S.C. § 1341 – Mail Fraud
Why applicable: Any component of the smurfing operation that involved use of the U.S. Postal Service (e.g., donor confirmation letters, campaign mailers based on fraudulent donor data) triggers this statute. Example application: Campaigns mailing FEC-mandated donor receipts to people who never made the donations.

8. 18 U.S.C. § 1957 – Engaging in Monetary Transactions in Property Derived from Specified Unlawful Activity
This is similar to § 1956 (money laundering), but applies to spending or transferring criminally derived property valued over $10,000. Smurfed donations could qualify as "proceeds" from unlawful structuring or identity fraud. Example application: Campaign disbursements (e.g., TV ads, staff salaries) funded by laundered, unlawful Smurf donations.

9. 18 U.S.C. § 1030 – Computer Fraud and Abuse Act (CFAA)
Why applicable: automated donation software, bots, or spoofing scripts were used to access ActBlue or other platforms in excess of authorization to submit fraudulent donations, this

triggers CFAA. Example application: A campaign or vendor scripts donations using saved payment credentials to inflate donor counts and launder money.

10. 18 U.S.C. § 1962 – Racketeer Influenced and Corrupt Organizations Act (RICO)
Why applicable: If smurfing into campaigns is part of a broader pattern of criminal enterprise (multiple actors, coordinated use of wire/mail fraud, identity theft, money laundering), then RICO applies. Example application: A nationwide network of political operatives, fundraisers, and payment processors using the same laundering structure across campaigns and platforms.

11. The Bank Secrecy Act (BSA) is relevant and may be implicated in Smurfing operations involving political campaigns, especially when contributions are structured to evade thresholds that would otherwise trigger Suspicious Activity Reports (SARs) or other financial institution reporting duties. The GOP House Judiciary has already publicly announced there are thousands of SARs' reports by various banks on Smurfing.
The Bank Secrecy Act (BSA) 31 U.S.C. § 5311, enacted in 1970, requires U.S. financial institutions to assist government agencies in detecting and preventing money laundering and other financial crimes. This includes:
-Detecting structuring (breaking up large transactions to evade reporting requirements),
-Filing Suspicious Activity Reports (SARs) when unusual or potentially illicit activity is detected, and
-Reporting cash transactions over $10,000, or repeated smaller transactions that appear coordinated.
-While political campaigns and PACs are not directly regulated under the BSA, banks, credit card processors, and fundraising platforms like ActBlue or Stripe are. Smurfed campaign contributions are being routed through Stripe, ActBlue, Democracy Engine, merchant banking partners and others, those funds being structured to evade detection, then:
Structuring political donations to avoid financial reporting duties of BSA-covered entities may constitute a conspiracy to cause false reporting or non-reporting by a financial institution. ActBlue has received large volumes of small-dollar contributions that, on information and belief, were structured for the purpose of evading transaction thresholds and risk screening protocols imposed on financial institutions under the Bank Secrecy Act (31 U.S.C. § 5311 et seq.). Such contributions constitute violations of 31 U.S.C. § 5324 (Structuring) and suggest a broader conspiracy to avoid regulatory oversight by concealing the source, volume, and aggregation of campaign funds.

12. 31 U.S.C. § 5324 – Structuring Transactions to Evade Reporting Requirements
Criminalizes transactions designed to evade federal transaction reporting thresholds. It applies not only to cash, but also to wire and electronic fund transfers that are split up to avoid scrutiny. Example: A $50,000 donation is split into 500 micro-donations of $100 using synthetic donor identities. Each transaction stays below card processor internal flagging levels, evading anti-fraud thresholds and SAR triggers.

IV. Contributors to this Complaint:

Keith A Schneider (on X: @SmurfSearch), SmurfSearch Owner, Developer, Manager

Greg Sternbach (on X: The Dominator @PatriotsACT), IT Technician and Data Infrastructure Engineer

Peter Bernegger (on X: @ Peter Bernegger), Independent Journalist, President of Election Watch, Inc.

V. CERTIFICATION

Pursuant to 52 U.S.C. § 30109(a)(1), I hereby swear and affirm under penalty of perjury that the statements made in this complaint are, upon information and belief, true, correct, and complete to the best of my knowledge.

The facts set forth in this complaint are based upon careful analysis by myself, members of my team of experts, of publicly available Federal Election Commission data, Congressional investigation findings that are matters of public record, statistical analysis of contribution patterns using established methodological approaches, and documented evidence of contribution patterns that are impossible under any legitimate scenario.

I make this complaint not as a partisan political attack but as a concerned citizen who believes in the integrity of our election system. The victims of this fraud - thousands of elderly Americans whose identities have been stolen - deserve justice. The American people deserve elections free from criminal manipulation. The rule of law demands that these violations be investigated and prosecuted to the fullest extent possible.

Julie Seegers
Complainant

Julie Seegers

SWORN TO AND SUBSCRIBED before me this _28th_ day of August, 2025.
State of Wisconsin
County of Kenosha

Notary Public: Anthony Knox

My commission expires: April 16th 2025

[Notary Seal]

ANTHONY RICHARD KNOX
NOTARY PUBLIC
STATE OF WISCONSIN

AFFIDAVIT

The State of Wisconsin)
) S.S.
County of WI)

I, Theodore Greg Sternbach, of Kenosha, Wisconsin, being deposed MAKE OATH AND SAY THAT:

1. In June 2025, SmurfSearch researchers found that there were over 500 million donations with blank transaction type codes missing between 2015 and 2025 while examining individual donor details in the bulk downloaded transactions from the FEC public website. These totals could not be reconciled with the bulk data downloads loaded into SmurfSearch (a website that helps expose how money is laundered into political campaigns). When questioning the FEC support staff about this discrepancy, the FEC stated that the transaction type code field is not required on filing forms for donations under $200. Only transactions with properly filled-in transaction type codes are included in the bulk data files available for download from the FEC website. The FEC explained that it is on purpose to align with all historical campaign donation data back to 1975. To get all donation transactions, the FEC staff recommended downloading the full raw database dump backup files from the Amazon S3 bucket (a cloud based storage for the FEC database backup data). The backup storage is open to the public to analyze all donations, including those with "blank" transaction type codes. These are also known as uncategorized transactions. Downloading and assembling the raw database requires significant computer processing power and database expertise to accurately build and access the complete database for analysis..

STATE OF WISCONSIN
COUNTY OF WI

SUBSCRIBED AND SWORN TO BEFORE
ME, on the 21st day of August, 2025

Signature _____ (Signature) Theodore Greg Sternbach
(Seal)
NOTARY PUBLIC
My Commission expires:
12/29/2026

ELIZABETH A BENITEZ
NOTARY PUBLIC
STATE OF WISCONSIN

Informational Notes and Terms

These Comprehensive Smurfing Reports clearly demonstrate the enormous problem of Smurfing within our country's Election Industrial Complex (EIC), both at the Federal and State levels in ways that have negatively affected our elections.

Smurfing is said to be a sophisticated and non-arbitrary racketeering money laundering scheme involving stolen identities, wire fraud, bank fraud and elderly abuse which rapidly continues to grow and has wide-reaching consequences to our society. New Smurfs are regularly appearing when monitoring the fec.gov web site for updates. Full Accountability through prompt, honest, open and transparent (discovery inclusive) investigations must occur to expose and prosecute those who undermine the integrity of our elections.

The following information about the overall SmurfSearch web site is helpful in understanding this Report and the database used to build this report.

The SmurfSearch Analysis/Reporting Database:

- **FEC Transactions Data** – The database used to compile this Committee report and thousands of other similar Committee reports spans **10.25 years from 2015 through 2025-Jul-14.** All data used is actual FEC Contributor transactions. Data acquired from the following sources results in a total database of **801,273,628** records.
  - FEC website as publicly available bulk download zip files for each of the the 2 year cycles published as 2016, 2018, 2020, 2022, 2024 and 2026 (last downloaded **2025-Jul-14**). These datasets total to approximately **262,929,275** Million records. The FEC explicitly states that they are to be used for reasons, among others, Public Analysis.
  - FEC internal weekly database backup(s) acquired from the AWS (Amazon Web Services) Cloud using a URL provided by FEC Technical Support Staff. The FEC data backup used for constructing the database is from a download of **19-May-2025**. The backup was restored to a server. Identified within this database were massive numbers of transaction records with a type code that is Blank/Null. Approximately **602 Million** of these records were extracted and dated from 01-01-2015 to the most

recent available ie:**19-May-2025**. This record set was further reduced by eliminating all records with an EntityType code NOT equal to 'IND' (INDividual Contributor) (approx: **72 Million**). These remaining **538,344,353** records were then included into the SmurfSearch Analysis/Reporting database.

- This full database consists of **801,273,628** Contributor Transactions net summed to **$64,286,905,339.72** USD. Note that because this dataset contains negative values it may be helpful to know that there are **2,819,471** transactions with Negative values totaling **($790,585,750.64)** USD along with **793,138,755** Positive value transactions totaling **$65,077,491,090.36** USD and also notable is that there are **5,315,402** transaction records with $ZERO USD amounts.
- After the transactions data was loaded, another table was created and constructed to contain Unique Names (UNames, see below Contributors and AKA Names) all derived from the transactions. All of the transactions in the database were counted, sorted, collated, grouped and analyzed to generate various statistics, which were then assigned to each Unique Name resulting in approximately **33,135,921** actual unique contributors.
- **NO CENTS:** All transaction data that originates from FEC BULK Downloads, for reasons unknown, have NO CENTS. All transaction amounts are given in integer dollars. **After reporting this to the FEC, their incredible response is that they will not fix the issue.** Various checks of FEC Bulk Downloadable data going as far back as 2001 confirms NO CENTS. The FEC data description of the Bulk Downloadable transactions describes the AMOUNT field as being of type "NUMBER(14,2)"; the 2 meaning 2 place decimal allocation for CENTS. Yet the data delivered has all CENTS dropped. The result of this flaw is that there are unknown MILLIONS of lost, untraceable dollars. All transactions from $.01 to $0.99 appear as amounts of $0.00. An examination of this reporting database shows **5,315,402** transactions of $ZERO USD. **It's not unreasonable to assume that all transactions in the database could have had CENTS in their amounts and therefore the total LOST DOLLAR valuation of these transactions is likely in the tens of millions of USD.**
- **BULK DATA Unexpectedly Changes:** FEC Bulk downloadable datasets are provided per USA 2 year election cycles. Simplistically, Contributor data is reported to the FEC and loaded into the FEC database and periodically BULK Datasets are produced for public consumption. As each 2 year cycle comes to closure, committee's

finish their data reporting to the FEC, the Bulk Downloadable datasets should stabilize. The older the data the more stable the expectation. This Reporting database was originally built on Bulk Datasets initially downloaded approximately Mid April 2023. The database was then updated in 2025 to add Bulk datasets going backwards to 2015/2016 and forward to 2023/2024 (keeping original bulk datasets intact) and the partial dataset for 2026 (effectively through **2025-Jul-14**). When comparing current Bulk datasets with the same datasets used in April 2023, it was discovered that the current FEC 2019/2020 Bulk dataset had dramatically changed. It was determined that sometime after April 2023, the FEC changed the 2019/2020 Bulk Dataset by ***REMOVING 29,303,614*** transaction records. ***An examination of the "Missing" data shows this affected 66 committees and net summed to $2,355,884,759 USD. Of the 29 million Missing records, 26,996,348 of these are all from committee "C00694323" -- WINRED. These records when net summed total to: $1,603,039,615 USD.***

Click HERE for more information about this missing data.

- **INTEREST IN BLANK TRANSACTION TYPE RECORDS:** Over years of studying FEC data at the FEC web site, it is observed that there are unexplained numbers of transactions that indicate NO Transaction Type Code. This Analysis database has a total of **801,273,628** transactions and **538,344,353** Blank TrxType Transactions. The percentage of the Blank TrxType Transactions to the total Transactions is approximately **67.1**% vs: the percentage of the Public Bulk Downloadable Transactions of **32.8**%. It was learned from the FEC that they referred to these records as UNCHARACTERIZED and they were unsure how to handle them. In any case, they *never* made them openly available to the public like the Bulk Download data. **A *very serious issue* with these UNCHARACTERIZED Transaction records is that when compared to the *Publicly Available* Bulk data, over the same time period, these records number approximately 204.7% *more* records than Bulk data. When the above mentioned 72 Million excluded records are factored into this percentage, this *increases* the concealed transactions to exceed 230%. The public seems to be seriously deceived in that the Bulk data provided for 'Public Analysis' is massively incomplete.**

Click HERE for more information about this concealed data.

The following Terms/Column Headers generally apply to FEC Statistics. These apply to all summary data tables (pages) within the web site and this Report.

- **Smurf** – A generalized term used to refer to a specific 'Contributor' whose identity has been allegedly stolen to make fraudulent donation transactions to one or more FEC committees. It is important to note that a Contributor may have made some of the transactions attributed to their name, but for purposes of this report, all 'Contributors' listed within this report are alleged *Smurfs (noun)* as their transactions are unusually high frequency donors that often characterize a *Smurf*, among other distinctions. They are then said to be *Smurfing* (verb). The term itself originates from law enforcement agency(s). When any given transaction(s) becomes alleged to be fraudulent, the owner of such transaction(s) then is referred to as a *Smurf*. In the reporting database all contributors have a statistics profile consisting of such items as Total Transaction Counts and Amounts, by Committee ID, day(s), year(s), min, max, averages and more etc to help identify patterns of frequent transaction abuse. A 'Contributor' is comprised of a Unique Name (internally called a UName) originating from a transaction sorting/grouping compilation process and zero or more A/K/A (algorithmically matched, "**A**lso **K**nown **A**s", alias) names. All derived from additional transactions with similar names and within matching State, City and similar Zip codes. Often, when a Contributor is used/abused via *Smurfed* transactions they may sometimes, be called *Smurfs* but in no way for the purpose of assigning guilt. Again, such 'Contributors' are themselves most likely a victim of *Smurfing* crime(s). For this specific committee **C00401224** report, there are **281,434** number of unames (*Smurfs*) detected as encompassing **178,204,660** alleged *Smurfed* transactions totaling **$3,543,266,360**. These transactions begin as early as **2015-01-01** continuing through as recent as **2024-12-31** spanning a period of **~10years2days**.

  Click HERE for a generalized explanation of "*Smurfing*" at Investopedia.com.

- **Contributor** – For purposes of this reporting database, this is a Unique Name (internally called a uname). It is internally assigned a unique ID number called a UID and that UID is linked to every transaction associated with that name. A uname also has associated with it zero or more A/K/A names internally called likeNames. Transactions associated

with each likeName are also inherently associated with the master Unique uname. Thus, when referring to a Contributor nearly always means all A/K/A names inclusive as a singular identity. See below for the description of A/K/A Names.

- **A/K/A Name(s)** – These are alias names that are found to be associated with a “Unique Name Contributor” (eg: “DOE, JOHN”). These are most often seen as simple variations to the 'Unique Name' (uname) such as “DOE, JOHN MR”. Contributor names also appear in random variations with Titles (eg: MR, MRS, DR, MD, COL, LT, ESQ), Middle initials, First or Last name Initials, hyphenated names and so on, all with or without punctuation etc. These important features of the SmurfSearch web site are that the totality of the available Transaction datasets are simply raw individual transactions and the finding/joining these disparate names together makes many transactions appearing separate, become a Individual Contributor. Sadly, the quality of the individual data in the databases varies greatly. Sometimes names that are supposed to be LAST, FIRST appear as FIRST, LAST with and without spelling errors, abbreviations, hyphenations, initials, titles, ranks, professions and many other variations make the aka name grouping effort imperfect. This author asserts that the compilation is sufficient and that a writ all success rate of name matching has been reasonably achieved. Of the **801,273,628** transaction records, the count of Unique Contributor names has been reduced to **33,135,921** where **30,377,436** are singular unique names and **2,758,485** have associated A/K/A Names totaling **4,163,225** at an average of **2.4** each. The largest number of A/K/A names associated with any of the Unames is **91**.
- **NTRX** – FEC_NTRX refers to the **Number of Transactions** totaled across the database, relative to a 'Contributor'. This number is used as a data-point among others that contribute to a donation statistics profile. A large NTRX count is a strong indicator of *Smurfing* activity.
- **CTRX** – FEC_CTRX is similar to FEC_NTRX except it is only a count of those transactions whose types are generally considered to be of an Individual Contribution character. For most names these two values are the same. Sometimes, CTRX is a subset of the NTRX value. Transaction Types such as the FEC "15C" type are not included in the CTRX count as they are more so used by Candidates for reporting such things as expenses (contributions to self). This count is used internally to help rule out contributions that may be construed as *Smurf* false positives. EG: A well known public figure has a large

NTRX count, but upon examination of their transactions, it became clear that a majority of their contributions are type 15C listing their limousine, air travel, dinners, fuel, parking etc as contributions to their own committee(s). Their CTRX count, lacking the 15C transactions can reduce their Contribution profile to a low rate. Note: These reports do not characterize the usage pattern of type 15C transactions and exclude them as they are not relevant to detecting *Smurfed* transactions. When the internal CTRX value varies from the FEC_NTRX value, it will be shown below the FEC_NTRX value in [ ] brackets.

- **TAMT** – FEC_TAMT refers to the **Total Amount** (in dollars) of all the (NTRX) transactions across the database, relative to a Contributor. This number contributes to the donation profile of a Contributor. Note that Negative Amounts affect this total due to mathematical summation.
- **MTBD** – FEC_MTBD refers to the **Max Transaction By Day** count of transactions across the database. It is a count of the Maximum Number Of Transactions executed **on any one day**, relative to a Contributor. This number contributes to the donation profile of a Contributor.
- **MABD** – FEC_MABD refers to the **Max Amount By Day** total dollars of transactions occurring within **any one day** across the database, relative to a Contributor. This Amount is unrelated to a Max Transactions By Day count. This number contributes to the donation profile of a Contributor.
- **TOT_AMT$, MAX_AMT$, MIN_AMT$, AVG_AMT$** -- These are the Total, Max,Min and Average Dollar amounts associated with a Contributor across the NTRX transactions belonging to a Contributor.
- **MAX_TBD, MAX_ABD** – These are the MAX Transaction Counts and Amounts, By Day associated with a Contributor. These data points contribute to the donation profile of the Contributor. Eg: A MAX_TBD=8 means that this is the highest count of transactions occurring in any single day. These 8 transactions may be to any number of different committees. An MAX_ABD=$100.00 means that the largest total donation(s) was $100.00 occurring on any single day. This may or may not be the same day as the MAX_TBD.
- **MSD CNT** – Refers to Multi-Same-Day Transaction Count(s). As a part of our Contributor profile data, we count all transactions that occur on any given day. The MAX of this is seen above as MTBD. However it can also refer to counts compiled within a view (eg: by CommitteeID) where

Contributions occur multiple times on the same day to a singular committee ID. For example, when reporting by Committee ID (ie: this report), MSD=1 means that there are two transactions on a day resulting in an MSD count of 1. A MSD=2 means there are 3 transactions on a day as the 2nd transaction is count 1 and the third transaction is count 2. A MSD=10 would mean 11 transactions in one day and so on. It must be noted here that **MSD CNT accumulates across all transaction days** within the reported dataset. Therefore, when multiple days of MSD counts occur, the totality of the value relative to a single day is lost. See MSD MAX.

- **MSD MAX** – Refers to the MAX number of MSD Counts occurring within a given singular day, within a CommitteeID for a given contributor. MSD CNT will show a count but it accumulates across multiple days. **MSD MAX** will show the **highest MSD Count that occurred on any one day within the dataset**.

ZIP Codes: Using a USPS freely downloadable Zip Code dataset of **42,735** codes, a cross check of all Transaction ZIP Codes was performed and there are **109,245** distinct zip codes used in the FEC database transactions. There are within the total reporting database, **67,168** unique invalid zip codes. Of the invalid Zip codes, some are blank and many appear as alpha/numeric gibberish, could be foreign codes or are unknown values. For this specific committee **C00401224** report, there are **2,015,871** transactions while the herein alleged *Smurfed* transactions number **462,147**.

Click HERE for more information about *Smurfing* Statstics within Zipcode regions.

States: The transactions in this analysis/reporting database list a total of **319** unique States codes. Some research shows that there are acceptable State codes recognized for other groupings such as USA, Territories, Freely Associated States (FAS), Commonwealth (CW) and Military (MIL). An effort was made to categorize all State Codes in a grouping called Affiliations. Affiliations are defined within this reporting database as "USA", "MIL", "TERRITORY", "FAS", "CW", "FOREIGN" and "CATCHALL". CATCHALL was used to group Blank states and other unidentifiable codes. All unidentifiable codes were *subjectively* grouped as FOREIGN or CATCHALL. Some of these State codes (eg: ZZ) are seen to specify Cities as "LONDON", "PARIS, "TIJUANA", "DEN HAAG" and more from everywhere. For this specific committee **C00401224** report, the number of States referenced in the transactions scanned is **74**.

Click HERE to learn more about States *Smurfing* Statistics and HERE to view this reports 'States Used Report'.

Counts & Amounts Formatting: Internal processing of these reports includes collecting Counts and Amounts as net *summed* totals as well as the counts of both Positive and Negative Transaction amounts. When you see a report column and or row cell data appearing with a value that appears as a number (count) followed by more numbers prefixed with P: and N:, this means that the count first shows a TOTAL (net summed) Trx count followed by a P: (positive trx count) and a N: (negative trx count). Similarly, when a column or a row cell involves Negative amounts (dollars), the cell would first show a Total (net summed) Trx Amount followed by a P: positive Trx amount and then followed by a N: negative Trx amount formatted within the () characters to indicate negative amounts per common accounting formats. Overall, it is sometimes important to be aware of contribution transactions that for reasons unknown, appear as negative values. These negative values when summed, affect the total such that it may appear lower than the total positive contributions.

Note: The statistical and summary data presented herein is compiled with the best effort to be accurate. The data obtained from the FEC presents many challenges when compiling statistics. There are many constraints such as blank or poorly formatted Names, Cities, States and Zip codes as well as invalid dates (zero dates and dates in the future). There are many States, Cities and Zip codes that are simply invalid. Names in the transaction records are mixed, misspelled and or backwards etc and we find what appears to be individuals having made transactions under variations of names (eg: DOE, JOHN and DOE, JOHN MR. etc). Of all transactions in the database, there are **174,680** Blank States, **66,251** Blank Cities and **4,313** Blank Names that when net summed, has a USD valuation of **$2,303,286.00**. When compiling the data, the only fields one can somewhat count on is that there is a Transaction Amount and a committee ID that the money flows to/from.

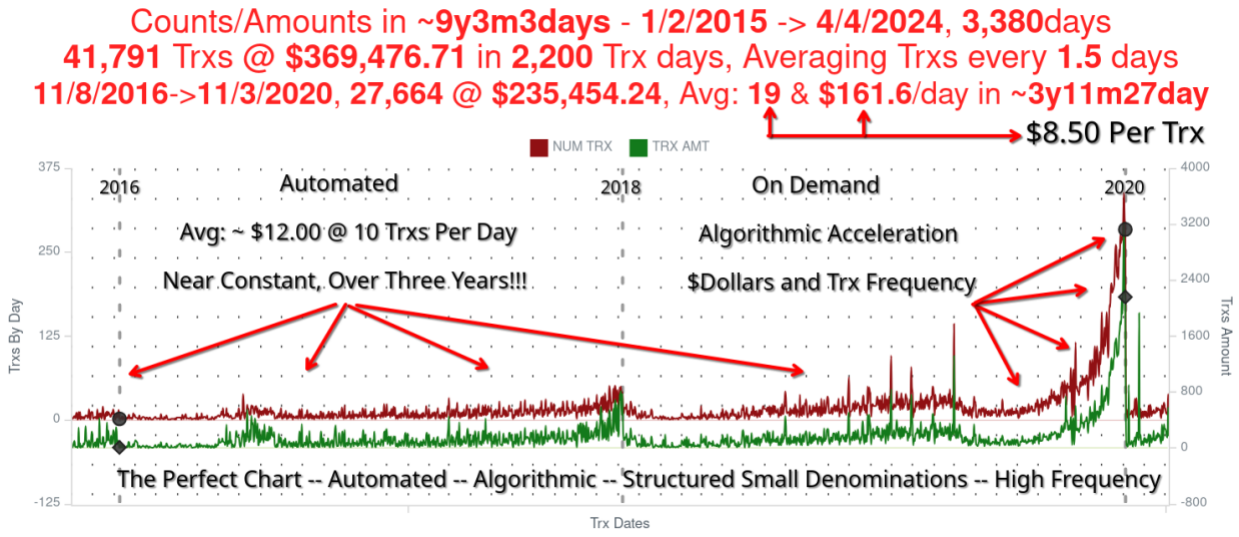
Where this compilation alleges wrongful activity, it is believed that the allegations simply demand Full Accountability through Prompt, Honest, Open and Transparent (Discovery Inclusive) Investigation(s).

<Prev - Next>

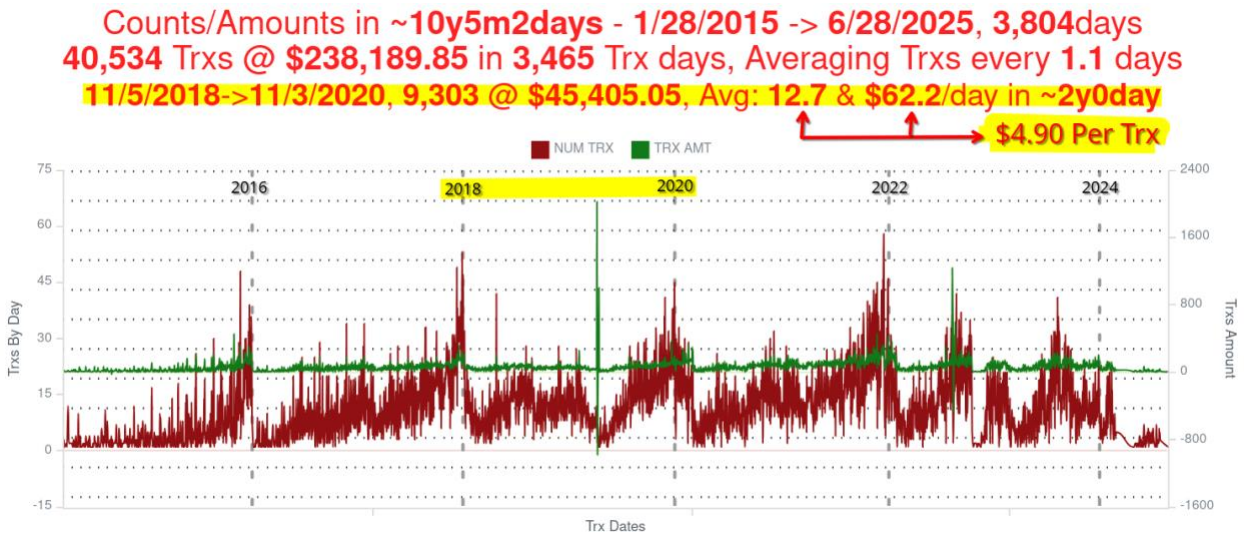
Charts Etc

The following charts show transaction execution profiles by dates for two *Smurfing* Contributors from the SmurfSearch database. Each illustrate High Frequency, High Volume contributions, Automated, Algorithmic transaction(s) execution, Structuctured Small Denominations including periodic Monthly spikes as well as what may be described as on-the-fly or "On Demand" scaling of the algorithm driven process.

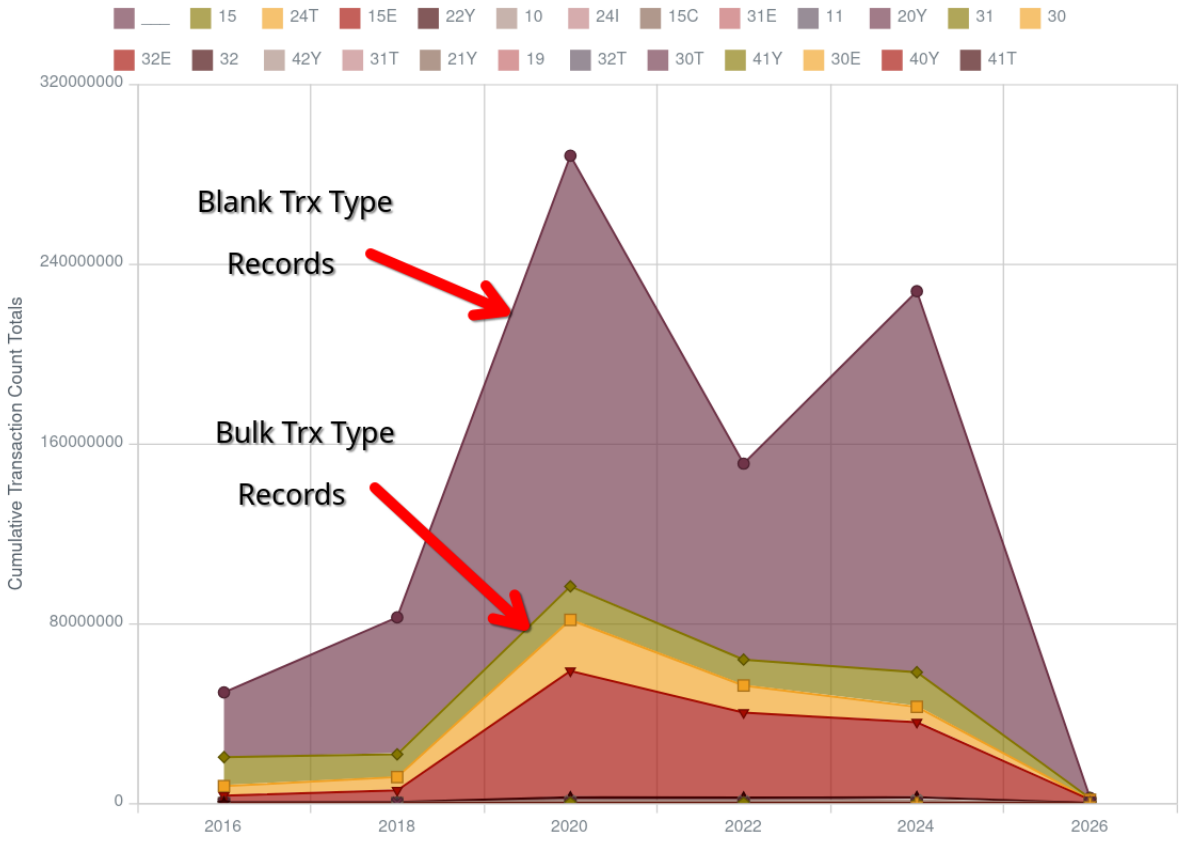
This chart illustrates all aspects to *Smurfing* including throttling of On-Demand Counts & Amounts as election(s) near. This Contributors profile indicates employment at a University.



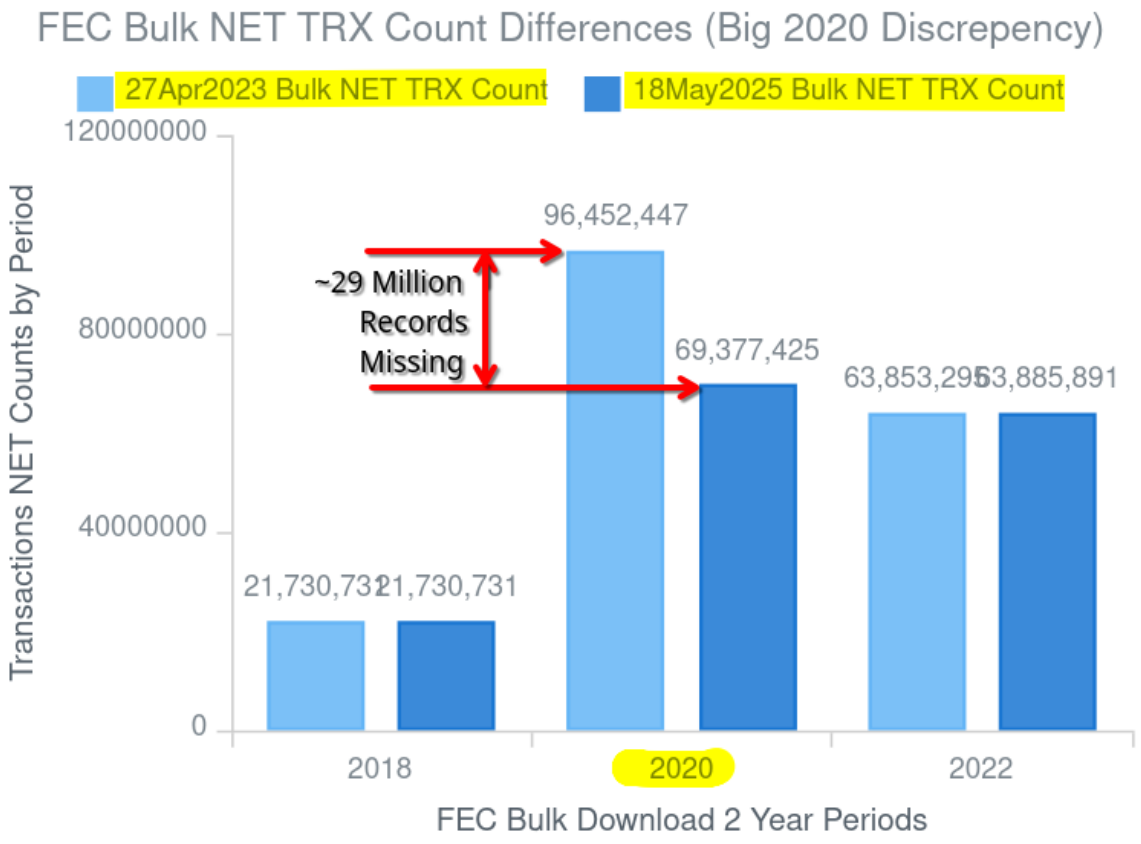
Note the heavy transaction counts and yet a comparitively steady amounts character. This Contributors profile indicates Retired since October 2015 from a legal profession.



This chart illustrates the 200%+ difference between the Uncategorized Blank Transaction Type records vs: the Bulk Transaction records visualized over 2 Year Election Periods.



This chart illustrates the scope of the Missing 29+ Million records from the 2019-2020 FEC Bulk dataset.



**** Credits ****

Many Thanks to the following:

- **Julie Seegers (on X: Julie S @jewelsHND)** for her relentless research and support of all things *Smurfs* and her aide to identify the kinds of tools/features needed to make such research possible for everyone.
- **Greg Sternbach (on X: The Dominator @PatriotsACT)** a skilled IT technician and Data Infrastructure Engineer, collaborated with FEC Tech Staff to restore a local replica of the full FEC database, enabling efficient extraction of over 600 Million Blank Transaction Type records. A major subset of this data was used to build the current SmurfSearch database along with other data analytics providing insight into smurfing patterns. All invaluable contributions.
- **H.O.T. Government (on X: @hotgovernment1)** for always being supportive.
- **The SOC** (Self Organizing Collective) of ***everyone*** along the way.

SmurfSearch is a website built in a Spirit similar to Free Open Source Software and is free to use. SmurfSearch is a work product of, managed & owned by Keith A Schneider (on X: @SmurfSearch) and the web hosting of such, is generously funded by Peter Bernegger owner of the electionwatch.info website and Electionwatch, Inc.