

LaShonda Greene – PPP Loan Fraud Conviction

Public Watch Records

Overview

LaShonda Greene was sentenced in 2022 after pleading guilty to orchestrating a sophisticated scheme involving fraudulent Paycheck Protection Program (PPP) applications during the COVID-19 pandemic economic relief rollout. Through a network of shell companies and falsified documentation, Greene successfully secured over \$3 million in federal funds meant for struggling small businesses before federal investigators detected the fraud pattern and initiated prosecution. Her case became one of the thousands of pandemic relief fraud prosecutions that collectively represented one of the largest instances of financial fraud against government programs in modern history.

Background on the PPP Program

The Paycheck Protection Program was established under the Coronavirus Aid, Relief, and Economic Security (CARES) Act signed into law on March 27, 2020. With an initial allocation of \$349 billion (later expanded), the program aimed to provide forgivable loans to small businesses to maintain their workforce during pandemic-related closures and economic disruption. Key features included:

- Loans designed primarily to cover payroll costs (at least 60% of funds)
- Additional allowances for rent, utilities, and mortgage interest
- Full loan forgiveness if employee retention criteria were met
- Minimal upfront verification to speed disbursement during crisis
- Administration through the Small Business Administration (SBA) and approved lenders

The program's rapid deployment, minimal verification requirements, and substantial funding created significant vulnerabilities to fraud, which individuals like Greene exploited.

The Criminal Scheme

Federal prosecutors detailed how Greene's operation worked:

Business Entity Creation and Manipulation

Greene established or claimed ownership of multiple business entities across several states, including:

- Five purported businesses in her home state
- Three additional entities registered in neighboring states

- Several "ghost" entities that existed only on paper

Most of these businesses either did not operate legitimate commercial activities or grossly exaggerated their operations, employee count, and revenue.

Documentation Falsification Techniques

Greene's fraud relied on sophisticated document manipulation:

1. Creation of falsified IRS tax forms, including Schedule C forms showing non-existent or inflated business income
2. Fabrication of payroll records for employees who did not exist
3. Manufacturing of bank statements showing business transactions that never occurred
4. Production of utility bills and lease agreements for business locations that were either residential properties or did not exist
5. Creation of backdated business licenses and permits

Loan Application Process

Between April 2020 and August 2021, Greene submitted at least 14 separate PPP loan applications to multiple financial institutions serving as SBA-approved lenders. She carefully structured the applications to avoid detection by:

- Using different lenders for each application
- Ensuring loan amounts varied but typically ranged from \$150,000 to \$350,000
- Staggering application submissions over time
- Using different bank accounts for fund receipt
- Creating unique email addresses and phone numbers for each business entity

Misuse of Funds

Rather than using the PPP funds for payroll as required by the program, Greene:

- Purchased luxury vehicles, including a Mercedes-Benz SUV and a Cadillac Escalade
- Made a down payment on a \$1.2 million residential property
- Funded personal investment accounts
- Transferred approximately \$1.1 million to personal bank accounts
- Purchased designer clothing, jewelry, and electronics
- Took multiple vacation trips during pandemic lockdowns

Detection and Investigation

The fraud was initially flagged through multiple mechanisms:

- Bank Secrecy Act suspicious activity reports filed by financial institutions
- Data analytics deployed by the SBA's Inspector General office that identified patterns across applications
- A whistleblower report from an employee at one of the lending institutions

The subsequent investigation, led jointly by the FBI, IRS Criminal Investigation Division, and the SBA Inspector General's Office, revealed the extensive nature of the scheme through:

- Execution of search warrants at Greene's residences and purported business locations
- Subpoenas of bank and financial records showing the flow of funds
- Interviews with individuals falsely listed as employees
- Digital forensic analysis of computers and devices revealing templates used to create false documents

Legal Proceedings and Sentencing

In early 2022, Greene was indicted on:

- 7 counts of wire fraud
- 5 counts of bank fraud
- 3 counts of making false statements to a financial institution
- 1 count of aggravated identity theft
- 1 count of money laundering

Facing overwhelming evidence, Greene entered into a plea agreement in mid-2022, pleading guilty to one count of wire fraud and one count of money laundering.

In November 2022, a federal judge sentenced Greene to:

- 78 months in federal prison
- 5 years of supervised release following incarceration
- Restitution of \$3.2 million to the Small Business Administration
- Forfeiture of assets purchased with fraudulent proceeds

During sentencing, the judge noted the particularly egregious nature of stealing funds intended to help struggling businesses during a national emergency.

Key Themes

Government Relief Program Exploitation

Greene's case exemplifies how emergency government programs designed for rapid deployment during crises often create vulnerabilities that opportunistic fraudsters can exploit. Key vulnerabilities in the PPP program included:

- Reliance on self-certification rather than upfront verification
- Pressure on lenders to process applications quickly with limited due diligence
- Limited cross-referencing capabilities between different government agencies
- Technology limitations for fraud detection at program launch
- Minimal staffing for oversight relative to program size

The case highlighted the tension between program accessibility during emergencies and program integrity.

Multi-Entity Fraud and Documentation Falsification

Greene's methodology demonstrated the sophisticated evolution of paper fraud in the digital age:

- Use of digital editing tools to create convincing forgeries
- Creation of complete fictional business ecosystems rather than single fraudulent entities
- Strategic dispersion of fraud across multiple jurisdictions and financial institutions
- Development of plausible business narratives tailored to pandemic conditions
- Careful attention to consistent details across multiple applications

This multi-entity approach allowed her to stay below thresholds that might trigger enhanced scrutiny while maximizing total fraudulent proceeds.

Pattern Consistency with Pandemic-Era White-Collar Crime

Greene's case aligns with broader patterns observed in COVID-19 relief fraud:

- Over 1,500 individuals were charged with PPP fraud between 2020-2023
- Total estimated fraudulent PPP loans exceeded \$80 billion according to the SBA Inspector General
- Common characteristics included shell companies, falsified payrolls, and identity theft
- Social media often provided evidence, with many fraudsters publicly displaying luxury purchases
- Geographic clustering of fraud cases suggested knowledge sharing among criminal networks

Her methods and the program vulnerabilities she exploited closely match those seen in thousands of similar cases across the country, suggesting systemic issues rather than isolated criminal opportunity.

Broader Implications

Program Design Lessons

The Greene case, along with thousands of similar prosecutions, prompted significant reassessment of emergency program design:

- Development of more robust real-time verification systems for future relief programs
- Creation of cross-agency data sharing protocols to identify suspicious patterns
- Enhancement of fraud risk assessment in program planning stages
- Implementation of tiered verification approaches based on risk profiles
- Investment in AI and machine learning tools for fraud detection

Law Enforcement Response

The unprecedented scale of pandemic relief fraud led to organizational changes in federal law enforcement:

- Establishment of the COVID-19 Fraud Enforcement Task Force in May 2021
- Creation of specialized prosecution teams focused on pandemic-related financial crimes
- Development of new investigative techniques specifically for relief program fraud
- Prioritization of high-value and multi-entity cases for prosecution
- Extension of statutes of limitations for pandemic fraud cases

Public Trust Impact

Cases like Greene's contributed to public skepticism about government program effectiveness:

- Reduced confidence in government's ability to administer emergency relief
- Political polarization around program integrity versus accessibility
- Calls for more stringent verification in future emergency programs
- Increased public awareness of fraud indicators
- Debate about the cost-benefit analysis of rapid deployment versus fraud prevention

Conclusion

The LaShonda Greene PPP fraud case stands as a representative example of how the unprecedented pandemic relief effort, while providing essential support to millions of legitimate businesses, also created opportunities for significant fraud. Her methods—creating multiple fictitious or enhanced business entities, falsifying extensive documentation, and strategically

approaching different lenders—exemplify the challenges faced by emergency programs that must balance immediate aid delivery with program integrity.

The case also demonstrates the federal government's commitment to pursuing and prosecuting pandemic relief fraud, even years after the programs have ended. As one of thousands of similar prosecutions, Greene's conviction forms part of what has become one of the largest anti-fraud efforts in American history, with investigations and prosecutions expected to continue well into the latter half of the 2020s.

For policy makers, the case offers valuable lessons about emergency program design, highlighting the need for scalable verification systems that can maintain integrity without creating overwhelming barriers to legitimate applicants during crisis situations.