HUMAN

Modern Fraud Threats in Government Relief Programs:

How Agencies Can Defend Against Cybercrime

By Joe Rogers, *Vice President of Public Sector at HUMAN Security*

A recent investigation by CBS News' "60 Minutes" has highlighted a significant issue: organized crime rings, often operating from overseas, are using stolen identities to steal billions of dollars from the U.S. Federal and State programs. These sophisticated fraud schemes specifically target public assistance initiatives, taking advantage of digital vulnerabilities and overwhelmed systems. The COVID-19 pandemic accelerated the delivery of relief funds, presenting new challenges for security systems still being implemented.

As these cyber-enabled crimes grow in complexity and scale, Public Sector organizations must evolve their defenses. HUMAN Security offers a modern solution that aligns with Public Sector standards and frameworks, like the NIST Cybersecurity Framework, to protect against automated fraud, account takeovers and bot-driven exploitation.

The Expanding Threat Landscape: Government Fraud at Scale

The fraud rings described in the CBS report do not fit the Hollywood stereotype of a lone hacker in a basement. These are industrial-scale operations run by criminal syndicates that:

- Use stolen or synthetic identities to apply for public benefits such as unemployment insurance, COVID relief, food assistance and housing vouchers.
- Leverage bots and automated scripts to rapidly test stolen credentials against Government login portals.
- Host phishing websites and fake document generators to fool verification systems.
- Exploit the lack of robust digital defenses in legacy Public Sector infrastructure.

At the height of the pandemic, the U.S. prioritized the rapid distribution of trillions in relief funds to support individuals and businesses in crisis. In the urgency to deliver aid quickly, some agencies adjusted standard fraud controls—creating unforeseen opportunities for bad actors. According to the CBS report, an estimated $280 billion was lost to fraud, with an additional $123 billion categorized as wasted or misused.

The tactics employed have now evolved into permanent tools of financial exploitation. Many cybercriminals continue to exploit social welfare and Government programs by leveraging automation and AI. Fraud isn't slowing down—it's scaling up.

Why Public Sector Agencies Are Attractive Targets

Government systems present a unique target profile for attackers due to a combination of high-value data, broad user bases and strained IT resources. Here's why the Public Sector is particularly vulnerable:

1. High Payout Potential

Each successful fraudulent claim can yield thousands of dollars in benefits. Fraudsters often operate in bulk, submitting thousands of applications using stolen identities.

2. Legacy Infrastructure

Many State and Local agencies still operate on outdated software stacks that lack modern bot detection or behavior-based threat analysis.

3. Lack of Real-Time Monitoring

Fraudulent applications often go undetected until after funds are dispersed. Manual review processes are insufficient to handle the volume of claims.

4. Increased Script & API Vulnerabilities

Fraudsters exploit front-end vulnerabilities, such as JavaScript manipulation or misuse of APIs, to simulate real user activity, bypass verification checks and deploy fake documents.

HUMAN Security: A Modern Solution for a Modern Threat

HUMAN Security specializes in protecting organizations from automated attacks, fraud and abuse by distinguishing between real users and malicious bots. HUMAN's solutions are uniquely positioned to help Public Sector agencies address the specific types of fraud exposed by 60 Minutes.

1. Bot and Automation Mitigation

Fraudsters frequently use bots to submit applications at scale, probe systems for weaknesses and conduct credential stuffing attacks. The HUNAN Defense Platform analyzes over 20 trillion digital interactions weekly to identify real-time anomalies.

Through behavioral analysis, device fingerprinting, and machine learning, we can help public sector clients:

- Detect non-human interaction patterns
- Prevent fake accounts from being created
- Block bot-driven denial-of-service or overload attempts

2. Account Takeover & Credential Abuse Defense

Many fraud schemes begin with access to a real person's Government credentials. We prevent account takeovers by identifying compromised credentials in real time and helping clients stop unauthorized login attempts.

Our Application Protection Package also integrates into public-facing login portals to block brute-force attempts and detect unusual login behavior.

3. Fake Identity and Synthetic Account Prevention

Fraudsters use fake IDs or generated synthetic identities to bypass identity checks. Our behavior-based analytics distinguish real users from fabricated personas—stopping fake account creation before it starts.

4. Real-Time Threat Intelligence:

By continuously monitoring emerging threats, we equip Public Sector clients with up-to-date information to counteract evolving fraud tactics.

5. Integration with Public Sector Frameworks:

Leading-edge solutions that align with standards like the NIST Cybersecurity Framework, HUMAN facilitates seamless integration into existing Government infrastructures and helps public sector clients with compliance and regulatory requirements.

Real-World Benefits to Government Agencies

By adopting fraud protection solutions, public agencies can:

- **Minimize Fraud Risk:** Real-time prevention minimizes the risk of sending funds to bad actors.
- **Protect Citizens:** Reduce identity theft and unauthorized access to sensitive citizen data.
- **Build Trust:** Demonstrating robust cybersecurity fosters public trust in digital Government systems.
- **Streamline Compliance:** Meet modern standards like PCI DSS 4.0 requirements 6.4.3. & 11.6.1 and NIST CSF with confidence.
- **Save Taxpayer Dollars:** Every fraudulent dollar blocked is money that can be returned to real beneficiaries or saved for future programs.

A Call to Action for Government Leaders

The fraud revealed in the CBS 60 Minutes report isn't an isolated event—it's a warning sign. Digital transformation has accelerated across public agencies, but fraud defenses haven't always kept pace.

Government leaders must take a proactive stance by:

- Modernizing fraud detection capabilities
- Closing visibility gaps across digital infrastructure
- Adopting behavior-based, real-time defenses like HUMAN Security
- Aligning security strategy with established frameworks (NIST, PCI DSS)

Fraud is no longer just a compliance risk—it's a national security issue. As public trust and taxpayer funds hang in the balance, Government agencies must embrace modern, intelligent and automated defense systems to keep fraudsters out.

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We verify that digital interactions, transactions, and connections are authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, please visit **www.humansecurity.com**