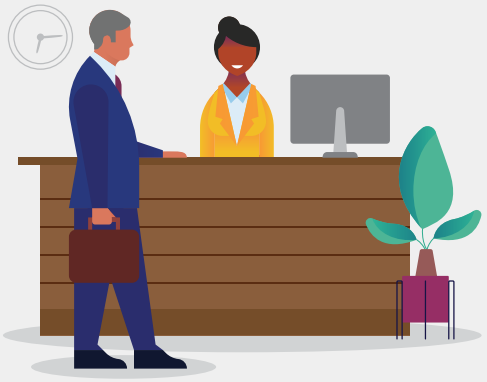
# Protecting Government Disbursements

How Prepaid Cards Can Help Mitigate Fraud

## Background

**COVID-19 and the resulting financial crisis endangered the health of billions of people around the world and distressed the economic health and wellbeing of tens of millions of people across the U.S.**

To address the crisis, state government agencies found themselves under unprecedented strain to deliver immediate and direct unemployment payments to workers and families impacted by COVID-19, as well as authorizing funds disbursement through the Pandemic Unemployment Assistance (PUA) program to those with hard-to-verify employment status, such as gig workers, self-employed or part-time/seasonal workers.[1] Unfortunately, that same loosening of eligibility requirements made it easier for fraudsters to apply and illegally obtain access to those benefit funds.



In the last year, **61 million** unemployment claims were filed through Nov 2020 (WSJ 2020)[2] and 885K unemployment claims peaked in one week in Dec 2020 (AP 2020), compared with an average of 230k in previous years.[3]

## How Unemployment Insurance Fraud Occurred

The sudden and unprecedented volume of pandemic related unemployment claims and the urgent need for quick delivery of benefit payments overwhelmed many state agencies and allowed organized criminals and fraudsters to exploit the process and fraudulently apply for these benefits. The following highlight the types of fraud associated with government programs:


### Application Fraud

Before a government payment is distributed, the agency managing the program must first determine an individual's eligibility for the benefit. Fraudsters obtain stolen personally identifiable information (PII) records and then use the stolen information to apply for government benefits. Stolen identities are obtained through various compromises and subsequently bought and sold on the cybercrime underground.

### Transaction Fraud

Approved applicants then receive their benefit funds either via prepaid debit cards or through direct deposits into an applicant-specified bank account. The funds are then taken off the prepaid card, either as manual cash or ATM withdrawals, or used by the fraudster to make illicit purchases and to effectively monetize or launder the funds.

### Double Dip Fraud

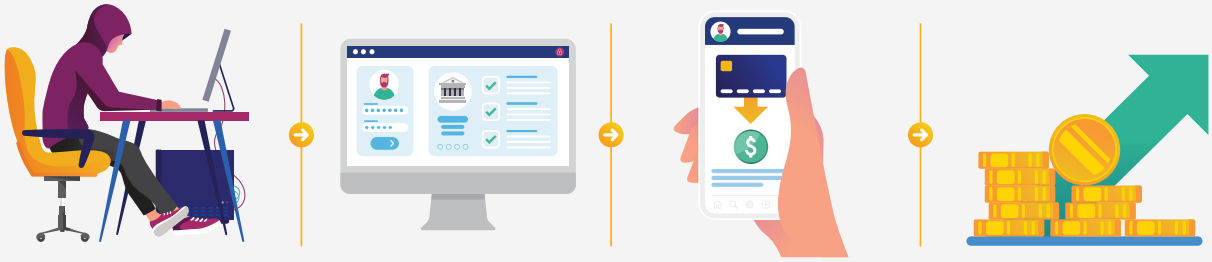
Once a prepaid card account has been established and funded using stolen identity, the fraudster can make a purchase using their government issued prepaid card, then file a fraudulent "unauthorized transaction" claim with the card issuer. The issuer returns the funds claimed as "unauthorized transactions" to the card while they investigate the fraudulent transaction claim. The fraudster retains the goods or services purchased using the original transaction and now has the refunded funds from the issuer which they can immediately use for additional transactions or cash withdrawals.

1. The fraud occurrences associated with the PUA are unprecedented and not reflective of general fraud risks within government-sponsored prepaid card programs.
2. Morath, WSJ.com, 2020, accessed 11/18/20, <http"//wjs.com/articles/how-many-us-workers-have-lost-their-jobs-during-corona-virus-pandemic-there-are-many-ways-to-count
3. Weisman, AP, 2020, Accessed 2/12/20, https://apnews.com/article/technology-jobless-claims-unemployment-coronavirus-pandemic-economy-3dfd19dfdf6a9e940b492e23b4d87403

# COVID-19-Related Government Program Fraud

Criminals have devised numerous methods for stealing government funds

## Transaction Lifecycle



Obtain stolen personal identifiable information (PII)

Submit online application for government COVID-19 relief programs

Receive funds via prepaid card or direct deposit to account created with stolen PII

Monetize funds

## How Prepaid Cards Can Protect Cardholders and Governments from Fraud

Prepaid card programs, and the financial institutions that issue the cards, are subject to strict regulation and oversight by numerous governing bodies. A number of programs and policies have been put in place to mitigate fraud on prepaid cards, where checks and direct deposits don`t provide the same protection.

### Cardholders

- **Federal Regulation E and Visa Zero Liability Protection:** Designed to protect consumers from unauthorized transactions. Cardholders are not liable for unauthorized purchases, if their card is lost, stolen or fraudulently used, online or offline.
- **Transaction Alerts:** Prepaid card programs generally allow cardholders to receive balance and other transaction alerts, check their real-time balance online, via text, email or by phone, and dispute unrecognized charges.
- **Freezing Accounts:** If a card is lost or stolen, cardholders can either choose to freeze their card account until they have retrieved their card or request a new card to be reissued.


Prepaid cards offer cardholders and government agencies more robust benefits and protection than checks or cash.

### Government Agency

- **Minimize Loss:** Provides government agencies the ability to freeze the card account thus preventing unauthorized cardholders access to any remaining/unused funds. A new card can then be requested to be reissued to the rightful owner. Checks and direct deposits on the other hand, do not offer the same protection.
- **Card Usage Data (portfolio level):** Access prepaid transaction data at the portfolio/program level to see when and how cardholders utilize their prepaid card (e.g., cash vs. purchase transactions, merchant segments, online vs. face to face, etc.), thus, providing agencies with valuable insights into possible fraudulent activity. No such usage data is available with checks or direct deposit.
- **24/7 Transaction Fraud Monitoring:** Continuous fraud monitoring that detects suspicious spend activity on the card. Funds disbursed via checks or direct deposit do not allow same level of monitoring.