



# Fraud Awareness and Prevention

June 8, 2016

Jamie Cutshaw  
Pay.gov Fraud Team

# Agenda

---

- What is fraud?
- Fraud threat landscape
- Fraud Risk Profile (FRP)
- What we can do
- What you can do
- Next steps for Pay.gov



# What is fraud?

---

- Wrongful or criminal deception intended to result in financial **or personal gain**
- Fraud Triangle elements:
  1. Motivation
  2. Rationalization
  3. **Opportunity**
- Waste and abuse
  - Inappropriate actions
  - Motives can be unclear
  - In government space, disruption is one common motive



# Fraud threat landscape

---

Fraud threats are:

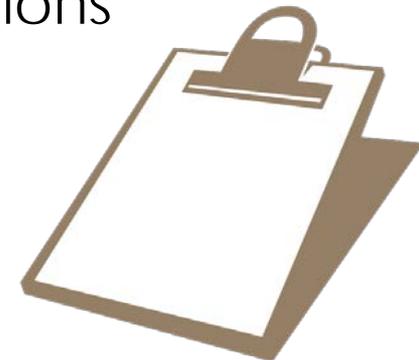
- Global
- Growing
- Multifaceted
- Ever-changing
- Internal or external
- Increasingly mobile
- Often unique to each agency



# Fraud Risk Profile

---

- Questionnaire to gauge application-specific fraud risks
- Risk factors include:
  - Customer base
  - Authentication level
  - Business type
- Data will be used to assign a risk classification and to determine whether additional controls are needed
- Other benefits include gathering information about:
  - Agency points of contact for fraud issues
  - Historical fraudulent behavior
  - Minimum and maximum dollar limits for forms
- Completed for roughly 75% of agency applications
- Questions may be sent to:  
**[ClevFraudRiskProfile@clev.frb.org](mailto:ClevFraudRiskProfile@clev.frb.org)**



# What we can do

---

- Continue to communicate with agencies
- Gather session data when users visit the Pay.gov site
- Leverage existing controls
  - AVS and CVV2 checks for card transactions
  - Review high-dollar ACH transactions (reject if fraudulent)
  - Monitor for blacklist data (user, account, IP address, etc.)
  - Block specific routing transit numbers or ACH accounts
  - Set minimum and maximum transaction limits on forms
  - Enforce user authentication on forms
  - Hide forms from the public
- Future enhancements
  - AVS improvements (to reduce false positives)
  - E-mail validation during self-enrollment
  - Vendor tool screening for high-risk transactions



# What you can do

---

- Request our Agency Guide to Fraud Management
- Ensure that your agency has completed the Fraud Risk Profile (FRP)
- For agencies that collect transaction data on their own websites:
  - Capture full billing address and CVV2 code (card-specific)
  - Collect user session data such as IP address
  - Enforce authentication
  - Validate user identities
  - Monitor for atypical behavior
    - Velocity of payments
    - Unusual payment amounts
    - Timestamp and geolocation of logged-in users
- If assistance is needed, contact Pay.gov Fraud Team at:  
**Clev.eGov.Fraud.Team@clev.frb.org**



# Next steps for Pay.gov

---

- Finish gathering and analyzing FRP data
- Know our customers (agencies)
- Implement additional controls for certain agency applications based on FRP risk classifications
- Continue to make fraud-related enhancements



# Questions

---

