Office of the State Treasurer

Mitigate Fraud: Ensure your Bank Account is Protected

FMC Annual Training Conference

Athens, Georgia

October 3, 2022

Impact of Payment Fraud on State Entities

- Fraudulent activity could impact banking relationships and increase costs
- Reputational risk to both the agency and the State
- Financial loss – fraudulent payments may not be recovered
- Potential audit findings

Web-based Application Issues

- **Compromised Web-based Accounts (CWA)** - Thieves gain access to make unauthorized transactions, including transferring funds, creating and adding fake employees to payroll, changing bank account payment information, and stealing sensitive customer information.
- Fraudsters are compromising web-based applications and attempting to initiate fraudulent transactions

- Web-based applications are allowing potential fraudulent user account set-up
- User accounts are being created by fraudsters without adequate verification
- Fraudsters are using this access to change bank account information and payment instructions

Payment Fraud Prevention

- For OST Bank Program accounts: check, ACH and wire fraud protection services will be required
- For non-OST Bank Program Accounts, fraud protection services are highly encouraged (talk with your OPB analyst)
- Please contact your banks to review and implement fraud protection services for all accounts
- Feel free to contact OST Banking for assistance
- Expect a memo from OST/SAO clarifying requirements

Payment Fraud Prevention

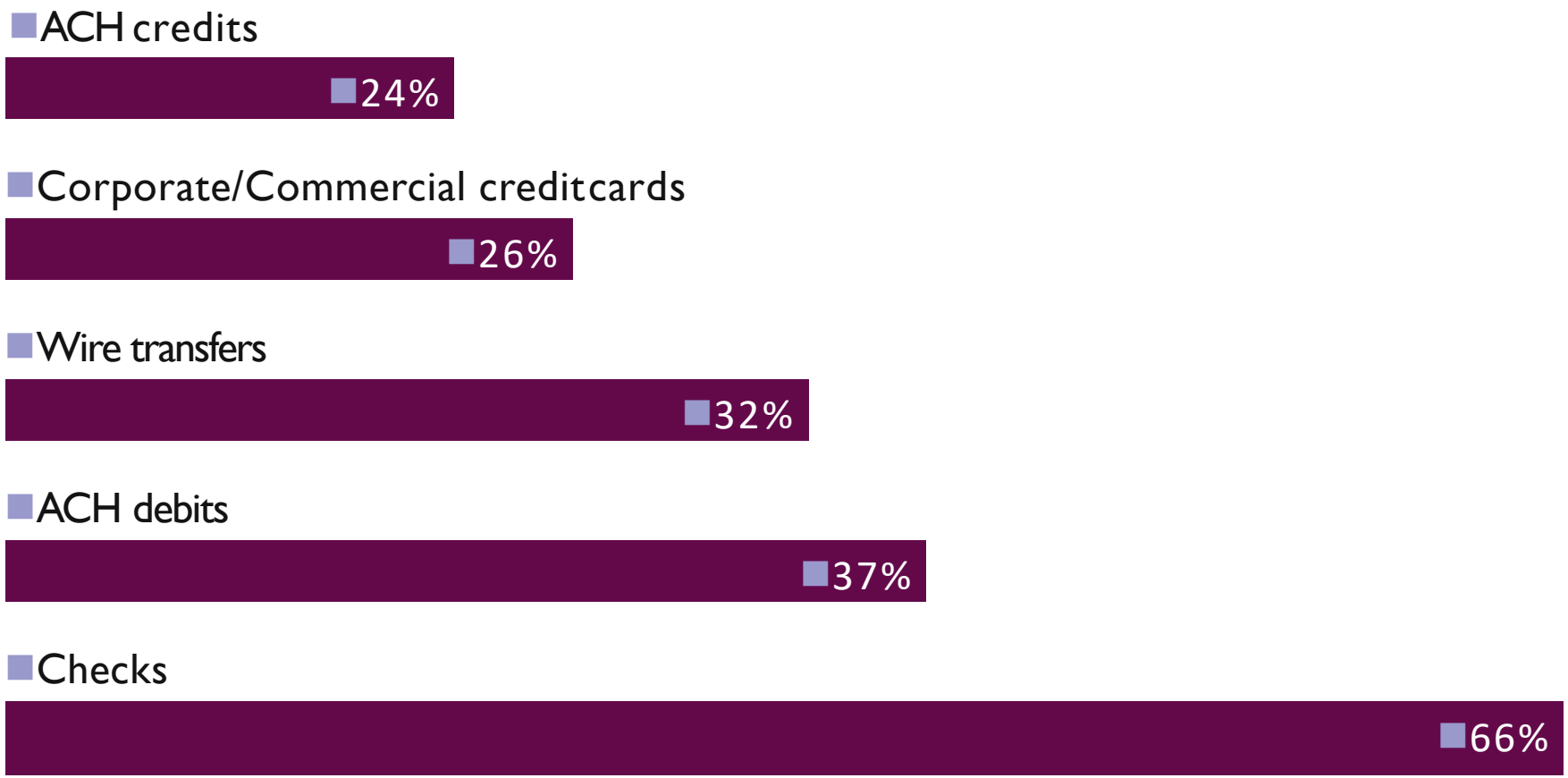
- This presentation will review payment fraud protection services by payment type (checks, ACH, wires).
  - Bank services for each type of payment
  - Agency roles for each type of payment

- At the end of my presentation, Richard Schneider, Deputy Inspector General, will discuss how to report fraud.

Reduce fraud related to payments

Are your payments a target for fraud?

Organizations that experienced fraud in 2021 by payment type



Source: Association for Financial Professionals, 2022 AFP Payments Fraud and Control Survey

Check Fraud – Bank Services (Fraud Reduction)

- Positive Pay identifies fraudulent checks by having the bank match presented checks against the Agency's check issue file
  - May want to add Payee Name verification service
  - Reverse Positive Pay (if a daily check issue file from the agency is not appropriate, bank can provide)

- ACH Block – if the account only allows for check payments

Check Fraud – Agency Roles (Fraud Reduction)

- Actively manage agency check issue file (timely and correct)
- Review exception items reported by the bank and instruct bank to pay or return
  - Review and decide within cutoff period
  - Know the default rule for lack of timely response
- Segregation of accounts
- Daily reconciliation

ACH Fraud – Bank Services (Fraud Reduction)

- ACH Fraud Filter identifies potentially fraudulent ACH transactions. Banks provide notification to agencies of any unrecognized ACH transactions
- ACH Fraud Filter can store company (payee) ID's that are authorized to debit agency bank accounts
- Agencies have the ability to allow or decline all (debit or credit) suspicious ACH transactions.

ACH Fraud – Agency Roles (Fraud Reduction)

- Vendor validation process for new or updated relationships
- Perform daily monitoring and reconciliation
- Limit transaction amounts, establish segregation of initiator and approver roles
- Review and approve ACH files before releasing to the bank
- Review suspicious items reported by the bank and instruct bank to allow or decline
  - Review and decide within cutoff period
  - Know the default rule for lack of response

Wire Fraud – Bank Services (Fraud Reduction)

Best Practices:

- Same-day, online reporting (pending, cleared, etc.) for wire activity
- Multifactor Authentication required for online banking platform access (Fobs, etc.)
- Ensure bank system provides for a System Administrator (agency) role that is robust and allows specific role assignments to facilitate segregation of duties, set wire dollar limits, and restrict use of free form wires

Wire Fraud – Agency Roles (Fraud Reduction)

- Limit use of wires to when necessary (expensive, hard to recover funds wired in error)
- Have strong controls around account validation of recipient
- No free form wires (use templates only)
- Segregate personnel authorized to approve templates from personnel authorized to initiate and approve wires
- Preauthorize dollar limits for wires (individual and aggregate limits)
- Perform daily monitoring and reconciliation
- (See: SAO Statewide Accounting Policy Manual)

Deposit Only Accts – Bank services (Fraud Reduction)

- These accounts can receive funds but do not make payments.
- Should have Auto Check return (check block)
- Should have ACH Block (block all ACH debits)
- Some banks offering these smaller, less active accounts may not have fraud prevention services available. Need to review risk (size of balances, etc.). Feel free to contact OST Banking for assistance.

Another Type of Payment Fraud Protection Service

- Account Validation Services (AVS) – provides status of account and account owner information prior to sending funds to an account.
  - Consult with OST Banking before proceeding.

General Methods of Financial Fraud

- Spear Phishing, Whale Phishing, Voice Phishing, etc.
- Business Email Compromise (BEC): Fraudster has taken over someone's email system.
- Online Account Takeover (ATO) Fraudster steals confidential information to access online accounts directly.

Basic Rules to Prevent Fraud

- Do not trust ANYONE
- Do not trust ANY Communication
- ID risky payment actions (initial account validation, changing account numbers, etc.) and ensure verification as appropriate (dollar thresholds, reputation risk, etc.)

Review Effectiveness of Controls

- **Ensure** controls are designed effectively and operating throughout the year
- **Review** your account creation processes for your web-applications
- **Assess** user provisioning policies and procedures
- **Strengthen** payment validations policies and procedures
- **Enforce** security awareness training programs
- **Confirm** agency staff is trained and following protocols, policies and procedures
- **Update** controls on a regular basis

OST Banking Contact Information

OST Banking Group:

ostbanking@treasury.ga.gov

OFFICE *of the* STATE TREASURER

Rhen Cain
Director of Banking Services
Office: 404-656-2171
Cell: 404-310-4448
rhen.cain@treasury.ga.gov

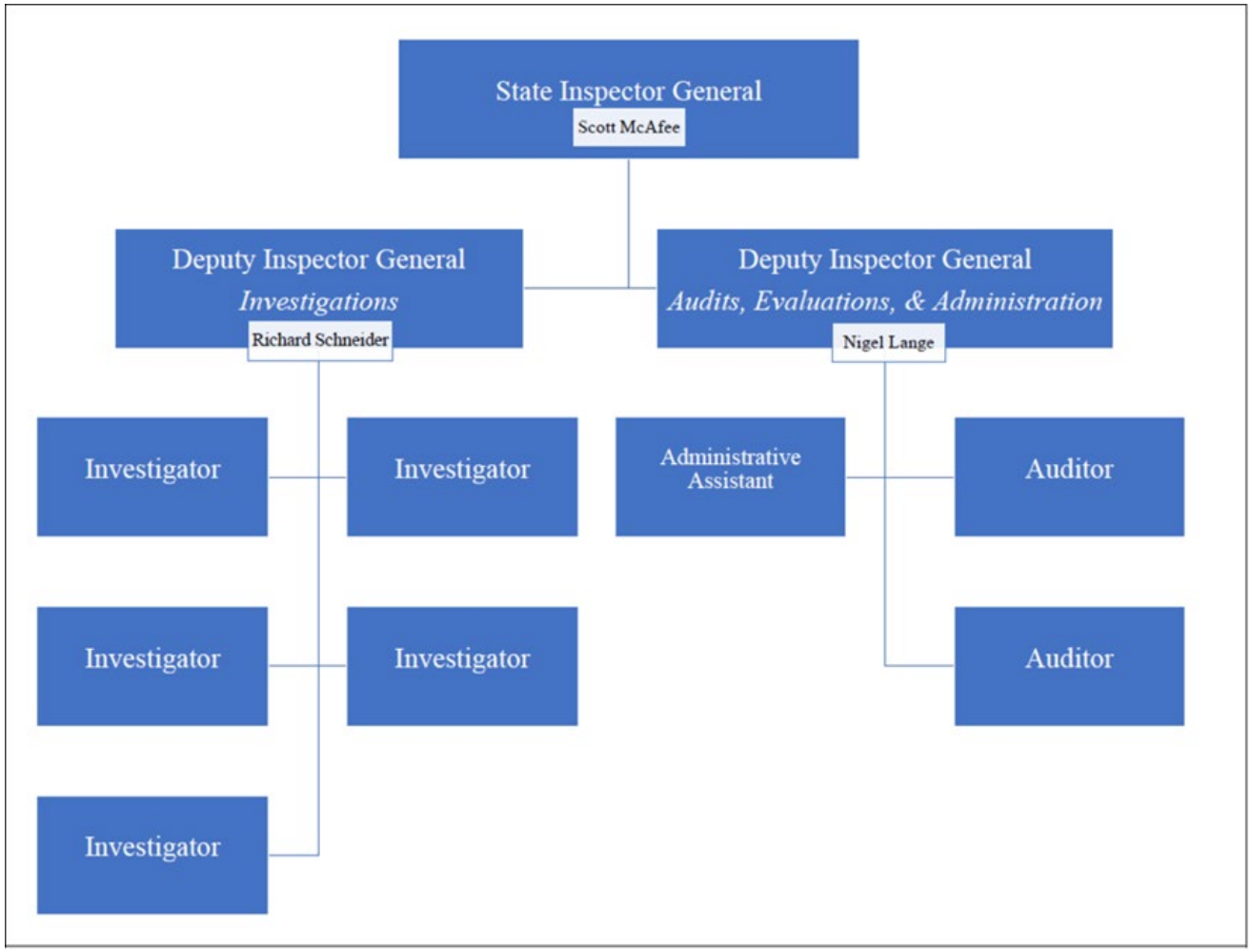
Jessica A. Smith
Banking Services Officer
Office: 404-232-7232
Cell: 404-436-3816
jessica.smith@treasury.ga.gov

Fraud Incidents – Follow up

Webinar Update

- Status Update
  - Treasury webinar from March 31, 2022

Changes at OIG



OIG Jurisdiction

- Allegations of fraud, waste, abuse, and corruption within the executive branch of state government.
- Fraud against executive branch agencies involving state funds or state administered federal funds.
- Allegations of ethics code violations.
- Oversight of sexual harassment investigations in state government.

Fraud/Waste/Abuse/Corruption Defined

- 'Fraud' means an act of intentional or reckless deceit to mislead or otherwise deceive.
- 'Waste' means a reckless or grossly negligent act that causes state funds to be spent in a manner that was not authorized or represents significant inefficiency and needless expense.
- 'Abuse' means the intentional, wrongful, or improper use or destruction of state resources.
- 'Corruption' means an intentional act of fraud, waste, or abuse or the use of public office for personal or pecuniary (financial) gain for oneself or another.

When/What to Report to OIG

- When fraud occurs related to your agency bank account.
  - Internal or External
- Any allegations of F/W/A, especially those with a financial component, affecting state agencies, state funds, or state administered federal funds.
- Unsure?
  - We maintain a current listing of internal investigative entities and can help direct your issue to the correct agency.

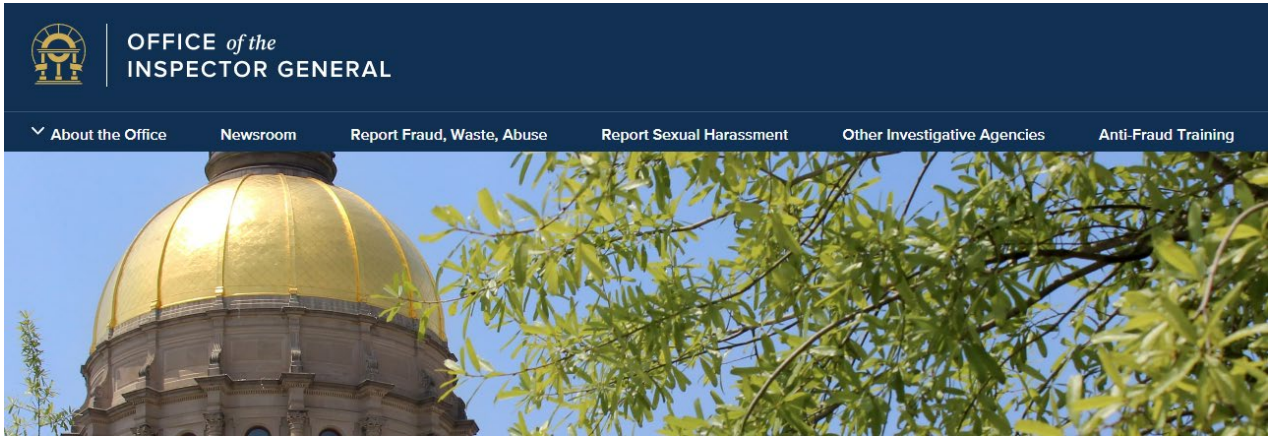
Reasons to Report to OIG

- Internal investigations may not be appropriate
  - Impartiality concerns/Conflict of Interest
  - Lack of financial investigative experience
- OIG will provide assistance to other law enforcement entities and work joint cases
- Identified internal control issues may affect other agencies
  - Enterprise approach
- Whistleblower Protection
  - O.C.G.A. §45-1-4
  - Identity Disclosure Protection
  - Retaliation Protection

Fraud Awareness Training

- We can provide free or low-cost training to your staff.
- Training is tailored to meet your needs or subject matter you are concerned about within your organization.
- Past Topics
  - Contract Fraud
  - Business Email Compromise
  - General Fraud Awareness
  - Ethics Training
- Request Form: https://oig.georgia.gov/anti-fraud-training-available-office-inspector-general

OIG Contact Information



- OIG Webform - https://oig.georgia.gov/report-fraud-waste-abuse
- OIG Email – inspector.general@oig.ga.gov

Richard Schneider
Deputy Inspector General
Mobile: 404-316-6274
richard.schneider@oig.ga.gov

Nigel Lange
Deputy Inspector General
Mobile: 404-317-6271
nigel.lange@oig.ga.gov

Questions?