Luke Collova
Underwriter
&
Geoff Boodell
Claim Counsel

# Employee dishonesty: how organizations can protect themselves

*December 4th, 2012*
*Thanks to: Clark County & Arthur J. Gallagher Risk Management Services, Inc.*

TRAVELERS

# *Important Note:*

- The views expressed in these materials are those of the author and do not necessarily reflect the views of The Travelers Companies, Inc. or any of its subsidiary insurance companies ("Travelers"). These materials are for general informational purposes only. In addition, this information does not amend, or otherwise affect, the terms, conditions or coverages of any insurance policy or bond issued by Travelers. This information is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law.
- This presentation is not intended to be a recommendation on the suitability of a specific insurance product for your operation. Please consult your agent or broker for advice.
- The information contained in this presentation has been compiled from sources believed to be reliable. Travelers makes no warranty, guarantee, or representation as to the accuracy or sufficiency of any such information. Travelers assumes no liability to any party for damages arising out of or in connection with the implementation of any recommendations suggested in this presentation.

# *Outline*

- Underwriting employee dishonesty exposure: what can be learned?
- Employee theft statistics
- Insurance coverage
- Geoff: Claims perspective
- Questions

# Underwriting Guidelines and Rating Parameters

- Type of business
- Size of business
- Multiple locations
- Number of years in business
- Internal controls
  - Segregation of duties, for example bank statement controls and reconciliations
- Loss experience
- Hiring practices
  - Employee screening, background checks
- Financial performance
- External controls
- Employee count
- Limit
- Retention/deductible

# *Internal Controls / Loss Prevention Program*

❑ Hiring practices
- ▪ Employee screening
- ▪ Background checks

❑ Segregation of employee duties
- ▪ Bank account procedures (for example, bank statement controls and reconciliations)
- ▪ Computer procedures
- ▪ Vendor/supplier procedures (for example registering, verifying and issuing payments)
- ▪ Dual control is key

❑ Internal Audits

❑ External Audits

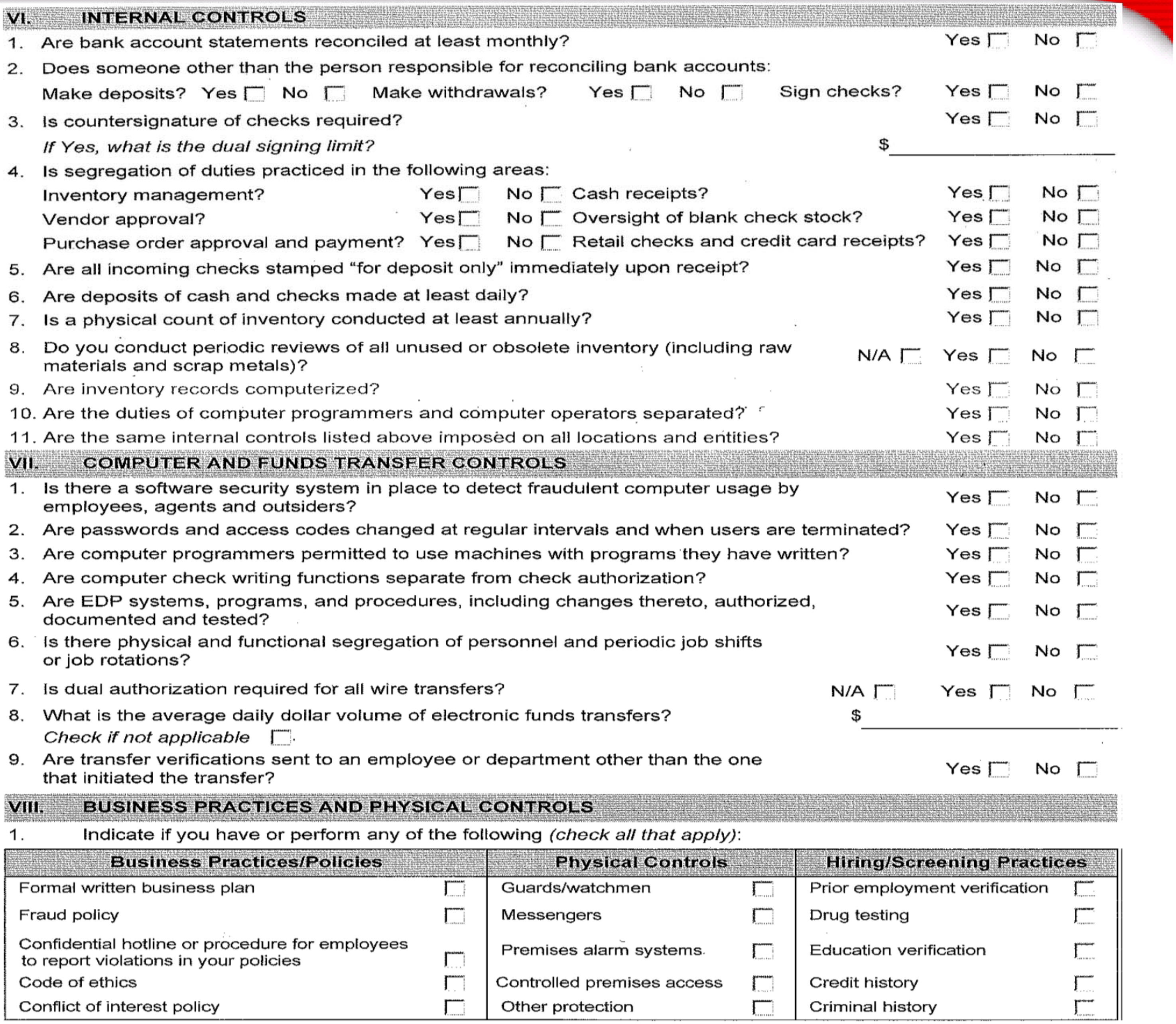
❑ Internal Security

❑ External Security

# Financial Performance

- Good times
  - Stability of funds – business as usual with full processes in place
  - Stability of staff – positions all filled, moral is good and oversight in place
  - A time when business practices can be improved or solidified

- Tough times
  - Funds – cost cutting, processes consolidated or shortened
  - Staff – reductions, less segregation in duties and heightened fear
  - A time when a heightened focus should be put on existing buseiness practices.



## VI. INTERNAL CONTROLS

1. Are bank account statements reconciled at least monthly? Yes □ No □

2. Does someone other than the person responsible for reconciling bank accounts:
   Make deposits? Yes □ No □ Make withdrawals? Yes □ No □ Sign checks? Yes □ No □

3. Is countersignature of checks required? Yes □ No □
   *If Yes, what is the dual signing limit?* $ ______________

4. Is segregation of duties practiced in the following areas:
   Inventory management? Yes □ No □ Cash receipts? Yes □ No □
   Vendor approval? Yes □ No □ Oversight of blank check stock? Yes □ No □
   Purchase order approval and payment? Yes □ No □ Retail checks and credit card receipts? Yes □ No □

5. Are all incoming checks stamped "for deposit only" immediately upon receipt? Yes □ No □

6. Are deposits of cash and checks made at least daily? Yes □ No □

7. Is a physical count of inventory conducted at least annually? Yes □ No □

8. Do you conduct periodic reviews of all unused or obsolete inventory (including raw materials and scrap metals)? N/A □ Yes □ No □

9. Are inventory records computerized? Yes □ No □

10. Are the duties of computer programmers and computer operators separated? Yes □ No □

11. Are the same internal controls listed above imposed on all locations and entities? Yes □ No □

## VII. COMPUTER AND FUNDS TRANSFER CONTROLS

1. Is there a software security system in place to detect fraudulent computer usage by employees, agents and outsiders? Yes □ No □

2. Are passwords and access codes changed at regular intervals and when users are terminated? Yes □ No □

3. Are computer programmers permitted to use machines with programs they have written? Yes □ No □

4. Are computer check writing functions separate from check authorization? Yes □ No □

5. Are EDP systems, programs, and procedures, including changes thereto, authorized, documented and tested? Yes □ No □

6. Is there physical and functional segregation of personnel and periodic job shifts or job rotations? Yes □ No □

7. Is dual authorization required for all wire transfers? N/A □ Yes □ No □

8. What is the average daily dollar volume of electronic funds transfers? $ ______________
   *Check if not applicable* □

9. Are transfer verifications sent to an employee or department other than the one that initiated the transfer? Yes □ No □

## VIII. BUSINESS PRACTICES AND PHYSICAL CONTROLS

1. Indicate if you have or perform any of the following *(check all that apply)*:

| Business Practices/Policies | | Physical Controls | | Hiring/Screening Practices | |
|---|---|---|---|---|---|
| Formal written business plan | □ | Guards/watchmen | □ | Prior employment verification | □ |
| Fraud policy | □ | Messengers | □ | Drug testing | □ |
| Confidential hotline or procedure for employees to report violations in your policies | □ | Premises alarm systems | □ | Education verification | □ |
| Code of ethics | □ | Controlled premises access | □ | Credit history | □ |
| Conflict of interest policy | □ | Other protection | □ | Criminal history | □ |

TRAVELERS

# *Loss Prevention Program*

- It is important to understand the causes behind most claims in order to prevent them.

- 3 areas have been proven to be key factors:

1)Motivation
2)Rationalization
3)Opportunity (temptation)

# Employee Theft Statistics

## 2008 Report to the Nation on Occupation Fraud and Abuse Executive Summary

- 7% of annual revenues: $994 billion
- Median loss: $175,000
- More than 25% involve loss of at least $1 million
- Small businesses are especially vulnerable
- Two years to discover
- Anti-fraud controls are effective
- Red flag – living beyond their means

# *WHO ARE THE THIEVES?*

| | |
|---|---|
| Employees | 39.7% |
| Managers | 37.1% |
| Owners/Executives | 23.3% |

*(Based on Frequency of Cases)*

*Source: 2008 ACFE Report to the Nation on Occupational Fraud and Abuse*

# HOW MUCH ARE THEY TAKING?

## Median Loss, by Perpetrator Type

| | |
|---|---|
| ▪ Employees | $  70,000 |
| ▪ Managers | $150,000 |
| ▪ Owners/Executives | $834,000 |

*2008 ACFE Report to the Nation on Occupational Fraud and Abuse*

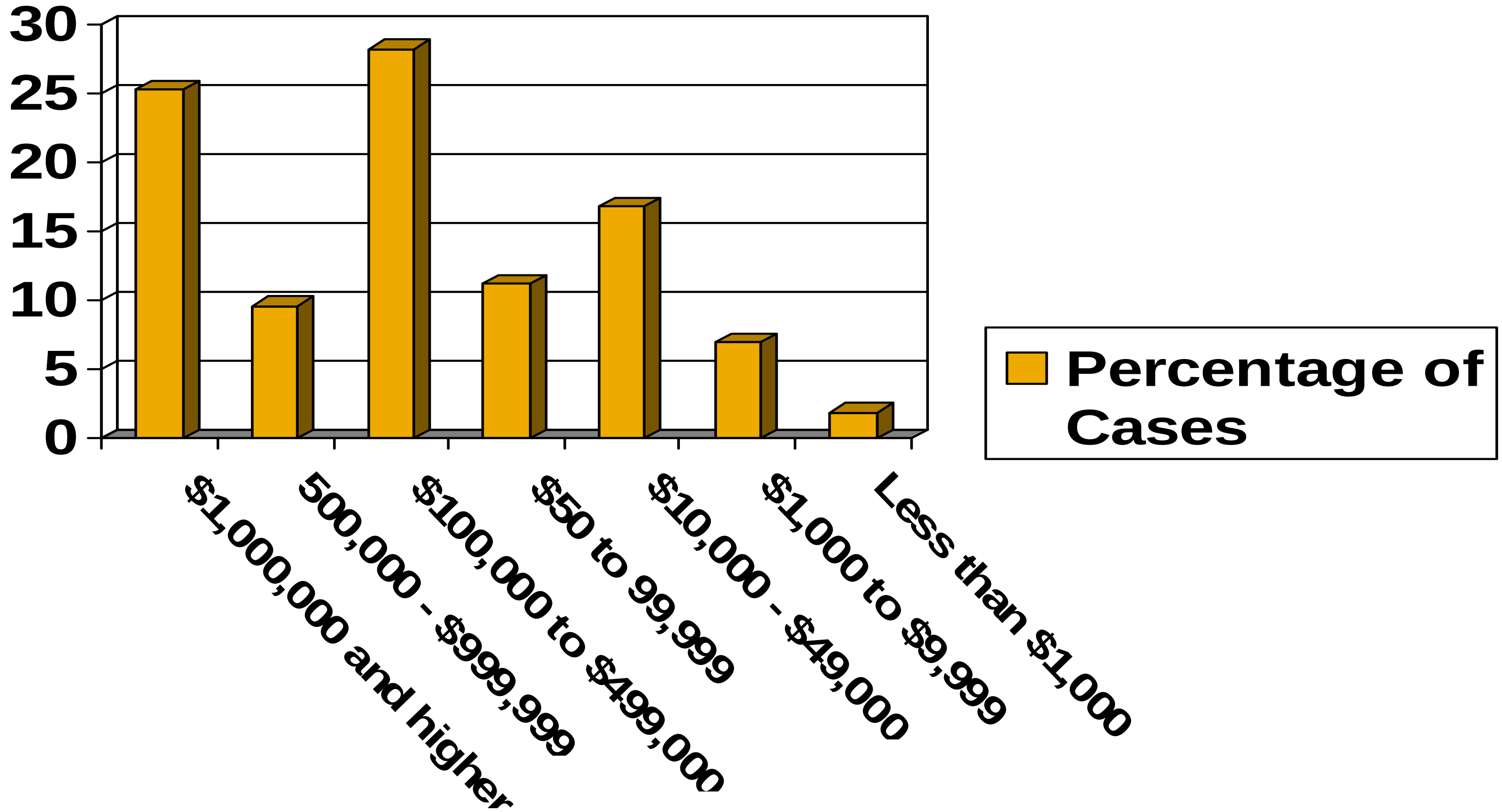
# WHAT ARE THEY TAKING?

Breakdown of Asset Misappropriations by Frequency

- 83.7% Cash (Includes Checks and Money Orders). Median Corruption Loss $375,000.
- 16.3% Non-Cash.  Median Loss $100,000.

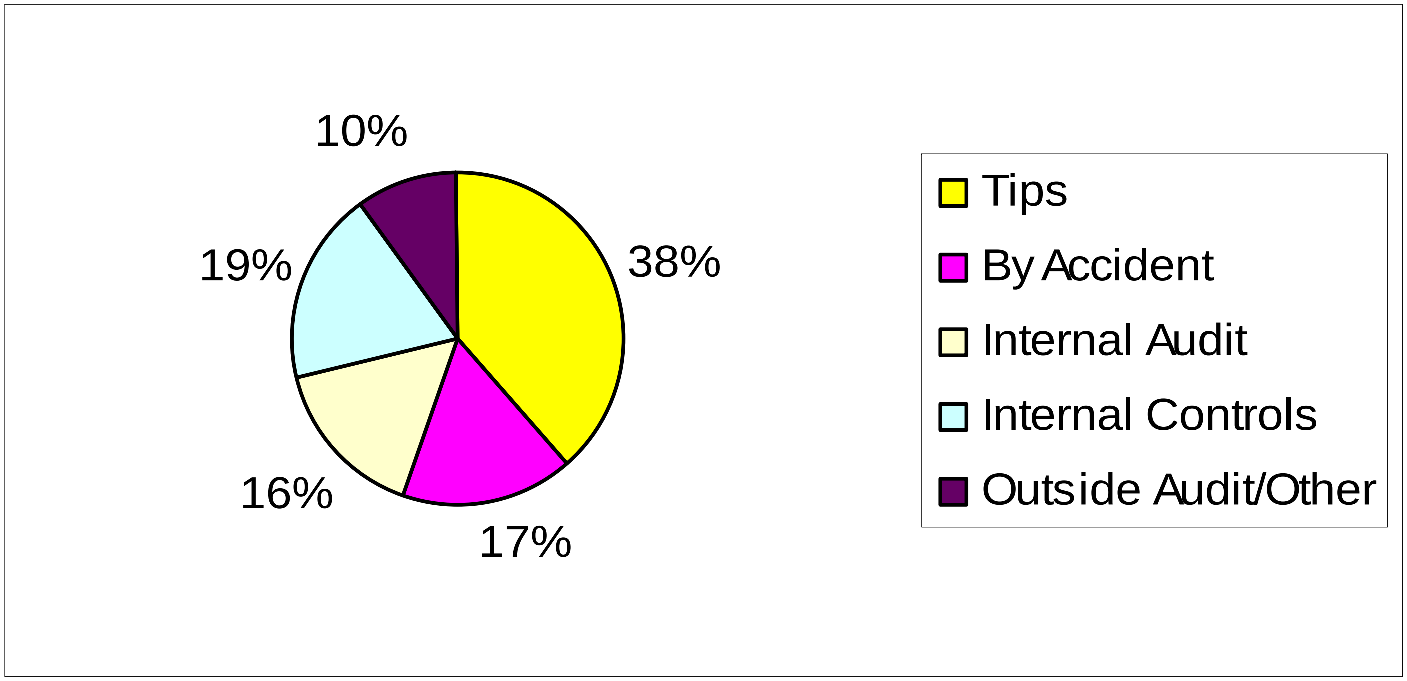
*Source: 2008 ACFE Report to the Nation on Occupational Fraud and Abuse.*
*(Median corruption loss figure excludes Financial Statement Fraud.)*

# Distribution of Dollar Loss



From the 2008 Report to the Nation on Occupational Fraud and Abuse

# 55+% of Discoveries Stem from Tips and Accidental Circumstances



*Source: 2008 ACFE Report to the Nation on Occupational Fraud and Abuse (adjusted to account for discoveries by more than once source.)*

# *Congratulations, you've caught the perpetrator!*

- **42.1% of firms recover NOTHING.**
- **23.4% recover 25% or less.**
- **Only 16.4% recover 100% of their loss, but these losses tend to be the smallest losses.**

** 2006 ACFE Report to the Nation on Occupational Fraud and Abuse*

# *What can employers do to help protect against this risk?*

- Establish a good loss prevention and internal control program

- Screen employees; maintain strong hiring practices

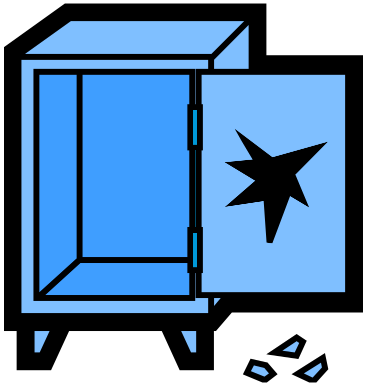
- Be ever-vigilant

- Purchase crime insurance

# INSURANCE COVERAGES

# Common Commercial Crime Coverages

- Employee Theft or Dishonesty
- ERISA Fidelity
- Employee Theft of Client Property (Third-Party)
- Forgery or Alteration
- Premises
- In Transit
- Money Orders and Counterfeit Money
- Computer Fraud
- Computer Program and Electronic Data Restoration Expense
- Funds Transfer Fraud
- Personal Accounts Protection for Forgery or Alteration
- Claim Expense



# Claim Example

An employee working for a timeshare company in Florida would go into the system and input fictitious renters. He would then authorize refunds towards the fictitious rentals, and divert these funds to his own personal bank account. Unrelated to these transactions, he was terminated, but the company neglected to change the system password or change the locks. The now former employee continued to perform similar transactions for the next six months. The loss was finally caught by auditors who noticed the refunds were going into one bank account.

Employee Theft covers the loss while he was an employee and for 30 days following his termination. Computer Fraud F covers the loss for the last 5 months as a non-employee.

# *Claim Example*

**A real estate developer issued a check dated 9/15. It was in the amount of $744,232 to the U.S. Treasury as payment for estimated taxes. The check was intercepted by an outside source. The date was altered to 10/15 and the payee was changed to “company X” The insured’s bank accepted the check and paid the check on 11/22 to company X.**

# Claim Example

**Over a 3 ½ year time span, a restaurant manager stole approximately $200,000 from his employer. The manager was improperly using the "delete" key when entering various servers' post-shift reports into the system and taking the amount of cash which was "deleted". This delete function was meant to be used only on rare occasions; such as when an improper order was placed.**

# *QUESTIONS?*

## VI. INTERNAL CONTROLS

1. Are bank account statements reconciled at least monthly? Yes □ No □

2. Does someone other than the person responsible for reconciling bank accounts:
   Make deposits? Yes □ No □ Make withdrawals? Yes □ No □ Sign checks? Yes □ No □

3. Is countersignature of checks required? Yes □ No □
   *If Yes, what is the dual signing limit?* $ ________

4. Is segregation of duties practiced in the following areas:
   Inventory management? Yes □ No □ Cash receipts? Yes □ No □
   Vendor approval? Yes □ No □ Oversight of blank check stock? Yes □ No □
   Purchase order approval and payment? Yes □ No □ Retail checks and credit card receipts? Yes □ No □

5. Are all incoming checks stamped "for deposit only" immediately upon receipt? Yes □ No □

6. Are deposits of cash and checks made at least daily? Yes □ No □

7. Is a physical count of inventory conducted at least annually? Yes □ No □

8. Do you conduct periodic reviews of all unused or obsolete inventory (including raw materials and scrap metals)? N/A □ Yes □ No □

9. Are inventory records computerized? Yes □ No □

10. Are the duties of computer programmers and computer operators separated? Yes □ No □

11. Are the same internal controls listed above imposed on all locations and entities? Yes □ No □

## VII. COMPUTER AND FUNDS TRANSFER CONTROLS

1. Is there a software security system in place to detect fraudulent computer usage by employees, agents and outsiders? Yes □ No □

2. Are passwords and access codes changed at regular intervals and when users are terminated? Yes □ No □

3. Are computer programmers permitted to use machines with programs they have written? Yes □ No □

4. Are computer check writing functions separate from check authorization? Yes □ No □

5. Are EDP systems, programs, and procedures, including changes thereto, authorized, documented and tested? Yes □ No □

6. Is there physical and functional segregation of personnel and periodic job shifts or job rotations? Yes □ No □

7. Is dual authorization required for all wire transfers? N/A □ Yes □ No □

8. What is the average daily dollar volume of electronic funds transfers? $ ________
   *Check if not applicable* □

9. Are transfer verifications sent to an employee or department other than the one that initiated the transfer? Yes □ No □

## VIII. BUSINESS PRACTICES AND PHYSICAL CONTROLS

1. Indicate if you have or perform any of the following *(check all that apply)*:

| Business Practices/Policies | | Physical Controls | | Hiring/Screening Practices | |
|---|---|---|---|---|---|
| Formal written business plan | □ | Guards/watchmen | □ | Prior employment verification | □ |
| Fraud policy | □ | Messengers | □ | Drug testing | □ |
| Confidential hotline or procedure for employees to report violations in your policies | □ | Premises alarm systems | □ | Education verification | □ |
| Code of ethics | □ | Controlled premises access | □ | Credit history | □ |
| Conflict of interest policy | □ | Other protection | □ | Criminal history | □ |