



This presentation was originally given by:

Larry A. Marks
PricewaterhouseCoopers

At the 2002 Windy City Summit

For questions about this material contact Larry at:

larry.marks@us.pwcglobal.com

FRAUD: AND YOU THOUGHT IT COULD ONLY HAPPEN TO THE OTHER GUY!

Arlen S. Lasinsky
Arlen.s.lasinsky@aexp.com
312/634-4743 Phone
312/634-5520 Fax

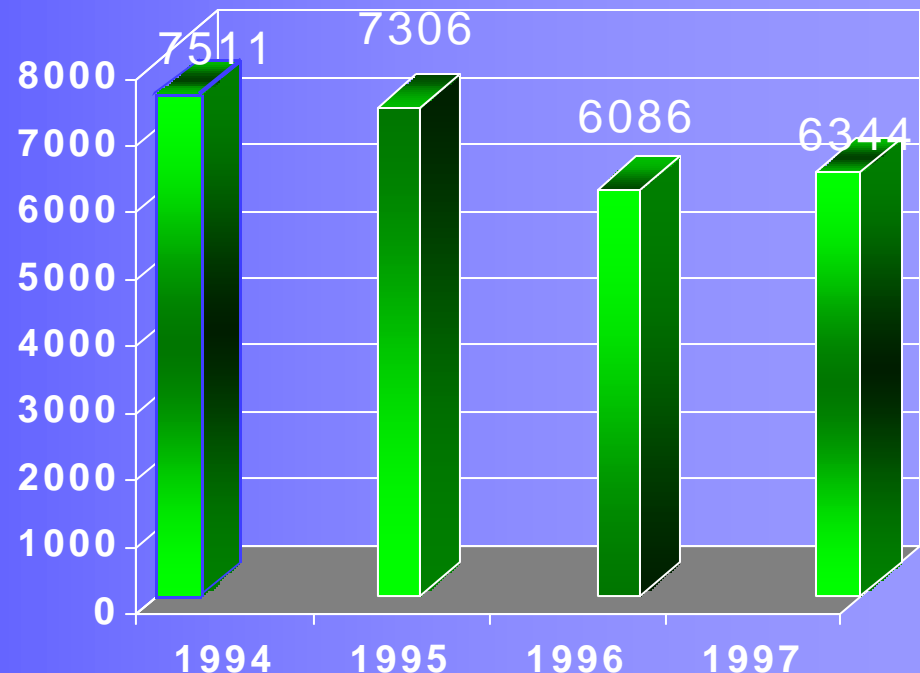
Larry A. Marks
larry.marks@us.pwcglobal.com
847/274-1945 Phone
847/432-8245 Fax



Check Fraud Perspective

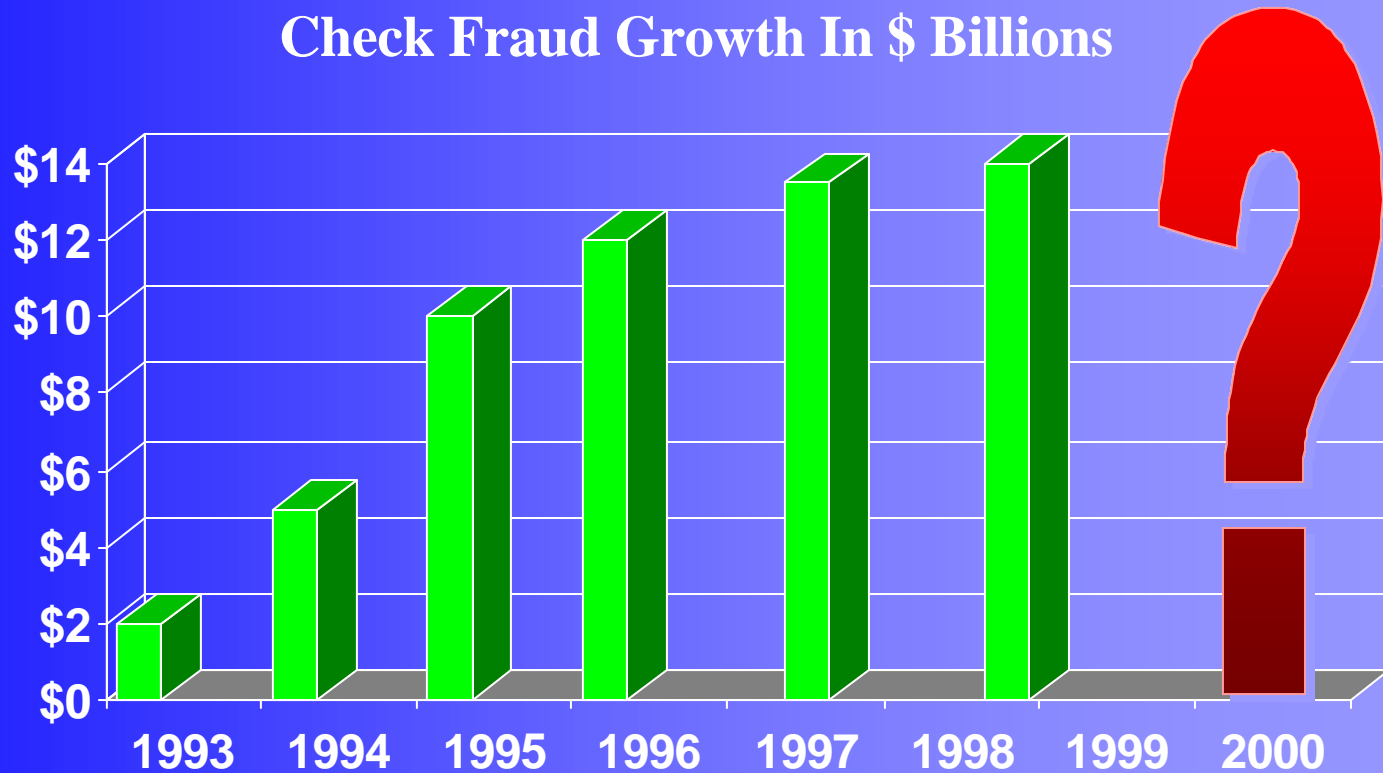
Throughout the 1990's there have been fewer bank robberies every year. Today there are fewer than 6,000 per year

- How much Check Fraud is there?



Check Fraud Growth

Check Fraud Growth In \$ Billions



Source: FBI



Why So Much Check Fraud?

- Big Payoffs!
- PC's
- Easy to use, “user friendly” software
- Scanners
- Color inkjet and laser printers
- Portable MICR encoding equipment
- Easy to obtain I.D. creation equipment



Will your people steal?

YES

NO



Who is the most likely to steal money from your company?

A hint, it is not the people working on the loading dock or the assembly line



Reasons for “Theft” (Borrowing)

- Angry at firm (They owe me this)
- Sickness in family
- Gambling losses
- Drug use (alcohol included)
- Out of control debt
- Divorce
- Greed



How Do the Bad Guys Get My Checks? Likelihood of Occurrence

Theft of check or image of check from vendor or supplier	Low
Return of goods for check refund	Low
Theft from U.S. Postal System	Moderate
Theft from your office	Higher
Purchased from one of your employees	Very High



Who Are the Invisible People in My Office?

- Cleaning staff
- Anyone with a faded white shirt, loosely knotted tie, pulling a “wheelie” with a black suitcase
- Messengers
- Employees
- The plant “lady” (man)



Let's Play a Game With Passwords



Most Commonly Used Computer Passwords

- Your first, last or kid's name
- "Secret"
- Stress-related words "deadline," "work"
- Sports teams or terms "Bulls," "Golfer"
- "Payday"
- "Bonkers"
- Current season, "Spring," "Summer"
- Your ethnic group
- Repeated characters "aaaaa," "bbbb"
- Obscenities, sexual terms
- Birthday of self, spouse, children,
- Wedding or graduation or other anniversary date
- Holidays
- Date of employment,
- Name of pet
- Phone number of spouse
- Name of child
- Street name
- School mascot or name



Source: Deloitte & Touche



Source: Marks & Associates

Where Passwords are hidden

- Taped to monitor
- Under keyboard
- In top right-hand drawer
- Under desk mat
- Written inside cover of dictionary or other book on desk
- In wallet



Identity Theft

1997 losses were \$745 Million

Costs to Financial Institutions are \$2 Billion

Stolen personal identifiers:

Social Security numbers

Driver's license numbers

ATM pin codes and cards

Telephone calling cards

Checks

Credit cards



How to Guard Against Identity Theft

- Don't carry extra credit cards, social security cards, or anything else with important data without a specific reason
- Remove your name from the marketing lists of credit reporting bureaus
- Install a locked mailbox and do not put outgoing mail in an unlocked facility
- Cancel all unused credit cards
- Order a credit report once per year
- Always save credit card receipts
- Create pin numbers that are “safe”



How to Guard Against Identity Theft

- Never print your Social Security or phone numbers on checks
- Carefully review credit card bills, bank statements and phone bills
- Don't throw away pre-approved credit card applications without tearing them up first
- Write checks with fine-point permanent markers
- Use electronic bill payment



CASE STUDY NO. 1

INTERNAL FRAUD

CASH RECEIPTS FRAUD

Facts of the case:

- Bookkeeper was crediting different accounts with cash receipts (Lagging)
- Lack of supervision
- Internal controls not in place
- \$750,000 embezzled in 3 months



CASE STUDY NO. 1

INTERNAL FRAUD

CASH RECEIPTS FRAUD

What Went Wrong?

- No proper supervision
- Lack of internal controls on the receivable side of the company-cash basis company
- Financial data not reviewed timely



CASE STUDY NO. 1

INTERNAL FRAUD

CASH RECEIPTS FRAUD

Procedures to Correct:

- Procedures to include receivables in the books and records
- Review of receivables on a more timely basis
- Proper internal controls
- Background checks



CASE STUDY NO. 2

INTERNAL FRAUD

LOST INVENTORY

Facts of the case:

- Inventory depleting – consumer goods
- Inventory received on the receiving dock removed
- Receiving dock employees driving BMW's
- Loss in the millions



CASE STUDY NO. 2

INTERNAL FRAUD

LOST INVENTORY

What was wrong with the controls?

- No security system
- Lack of internal controls pertaining to access to inventory
- No review of inventory levels on a timely basis
- Physical inventories only taken once per year



CASE STUDY NO. 2

INTERNAL FRAUD

LOST INVENTORY

How does it get fixed?

- State of the art security system or at least some type of security system
- Cycle counts periodically, preferably weekly
- Limited access to warehouse
- Proper documentation with respect to receiving inventory and other aspects of inventory
- Background checks



CASE STUDY NO. 3

INTERNAL FRAUD

CHECK FRAUD

Facts of the case:

- Controller had complete access to accounting records
- Authorized signer
- Recorded cash receipts, cash disbursements, prepared bank reconciliations
- Falsified documents, tax returns, and checks
- Millions embezzled



CASE STUDY NO. 3

INTERNAL FRAUD

CHECK FRAUD

Problems that existed:

- No proper supervision
- Lack of internal controls with respect to segregation of duties
- No internal inspection
- Owners did not participate in oversight



CASE STUDY NO. 3

INTERNAL FRAUD

CHECK FRAUD

Corrective Procedures:

- Proper segregation of duties
- Control over checks
- Control over receivables and cash receipts
- Owners need to be involved



POINTS TO NOTE

- Most thieves are not rocket scientists
- More than likely the thief will get caught
- Fraud is a crime of opportunity
- Personal fraud is on the rise



PROPER CONTROLS OVERALL

- Procedure manual
- Periodic review of procedures
- Segregation of duties
- Rotation of personnel in clerical positions
- Mandatory vacation
- Fraud hotline
- Background checks of new employees



CONTROLS INVENTORY

- Procedure manual
- Segregation of duties
- Physical counting of inventory
- Limited physical access to inventory
- Limited access to inventory records
- Proper documentation to receive and deliver
- Limited areas of receiving and shipping
- Surveillance controls



CONTROLS

ACCOUNTS RECEIVABLE

- Procedure manual
- Segregation of duties
- Limited access to receivable records
- Proper documentation for write-off
- Lock box for receivables
- Timely review of old balances
- Alert to customer complaints



CONTROLS DISBURSEMENTS

- Procedure manual
- Segregation of duties
- Limited access to check stock
- Positive pay
- Safety features on check
- Timely reconciliation of bank account
- Properly approved documentation



CONTROLS

WIRE TRANSFERS

- Procedure manual
- Segregation of duties
- Limited access to computer
- Proper approval via computer
- Repetitive wire transfers
- Dollar limit for wires
- Daily review of wires
- Monthly review of account analysis from Bank



CONTROLS INVESTMENTS

- Procedure manual-investment policy
- Segregation of duties
- Limited access to computer
- Proper approval via computer
- One account for funds-limited access
- Safekeeping of securities
- Monthly review of broker statements



CAN THIS HAPPEN TO YOU?

- Yes ! Don't kid yourself
- Remember, fraud is a crime of opportunity
- Most frauds surprise owners, top executives, etc.
- Frauds occur for many reasons
 - Personal financial problems
 - Medical bills
 - Drugs, alcohol or gambling problems
 - Disgruntled employees



How Do I Protect My Firm?

- Establish and document policies for all accounting functions
- Update and review the procedures with employees
- Conduct training
- Maintain segregation of duties
- Maintain physical security
 - check stock
 - signature plates / actual signatures



How Do I Protect My Firm?

continued...

- Conduct periodic reviews
- Communicate internally and externally with vendors
- Utilize bank products
- Screen new employees and temporary help
- Know your check printer
- Use fraud deterrent check stock
- Maintain separate accounts
- Reconcile accounts promptly



Who's Responsibility is it Anyway?

- UCC says that responsibility now rests squarely on the shoulders of both banks and check issuers!
- Fraud loss will more often be borne by the party who was in the best position to have prevented the fraud from occurring.



Responsibilities of the Company

- Exercise care in hiring and supervision
- Maintain sufficient internal security controls for check storage, issuance and reconciliation
- Examine bank statements within a reasonable time to detect fraud
- Evaluate and acquire appropriate fraud prevention / containment products - software, bank products
- Notify the bank immediately when fraud is suspected
- Consult your legal counsel for more information about your liabilities



Responsibilities of the Bank

- Banks must exercise ordinary care to prevent losses from counterfeit and forged items
- They must act in good faith in accordance with reasonable commercial standards of fair dealing
- Banks that act in good faith, and follow procedures similar to those of comparable banks, may not be found negligent for failure to detect fraud



Responsibilities of the Bank

continued...

Bulk Filing:

Since automated check processing is the standard in the banking industry and does not allow for inspection of signatures, under the revised UCC, banks may not be held liable for fraud loss simply because they did not inspect signatures on all checks.



Positive Pay As A Fraud Loss Deterrent

Three drawbacks

- Positive Pay does not have the ability to match the payee name on the in-clearing check with the payee name in the file sent to the bank. Sophisticated forgers know of this weakness and alter the payee name only. Altered payee names pose a very serious threat, but one that can be mitigated with high-security checks and secure name font
- Very few banks have linked the Positive Pay file to the teller line. Altered or counterfeit checks may be presented for payment at the teller window, and will likely get paid. All of America's largest banks are working on making this link, and a handful of banks have already done it. Note that the loss in this case is to the bank



Positive Pay As A Fraud Loss Deterrent

- The first check that matches the criteria in the data file will pay, even if it is a counterfeit check. The original check will become the “exception item” under review.
- Some organizations lack the technical expertise to create a file to send to the bank. Other organizations can, but their technology systems people are tied up on other “mission-critical” projects that take priority over Positive Pay (until a check fraud loss).



Protecting Paper Checks

Overt Security Features

- **Controlled Paper Stock** – Is your check paper available to forgers for making checks? Forgers often obtain original check paper by buying it from office supply stores, mail order catalogs or directly from most major check printers via 800 telephone numbers.
- **Watermarks** – Both true and artificial that cannot be copied or scanned.
- **Warning bands** – Are expected to draw attention to check security features and may deter criminals from experimenting. Are your warning bands properly worded?



Protecting Paper Checks

- **Type font size** – if printed too small or too light, type fonts can be erased and replaced with a new payee name or dollar amount

Laid lines – printed on the back of the check to deter cut-and-paste artists.

Sequenced inventory control number – printed on the back of un-numbered laser checks to account for all checks and to discourage employee theft of the blank stock.



Protect Paper Checks

Covert Security Features

- **Chemical-sensitive paper** – Reacts to chemicals commonly used to wash checks.
- **Copy Void Pantograph** – Voids the check when copied on most machines.
- **Microprinting** – Print that is too small for most scanners and copiers to capture.
- **Toner anchorage** – Chemical coating on laser checks that bonds the print toner into the paper, preventing alterations from the toner being lifted off with plastic tape.
- **UV light-sensitive fibers** – In the paper itself that become visible under UV light.



Bank Products That Help Prevent Fraud

- Account Reconciliation
- Positive Pay
- Sweep Accounts
- Automatic Transfers
- Lockbox
- ACH
- Pay Card
- Purchase Card
- Automatic Investment
- EDI

