Controlling Purchasing Card Risk

December 2, 2014

Alan. J. Goldberg, CIA, CRMA, MBA
Triplet Advisory Services

Overview

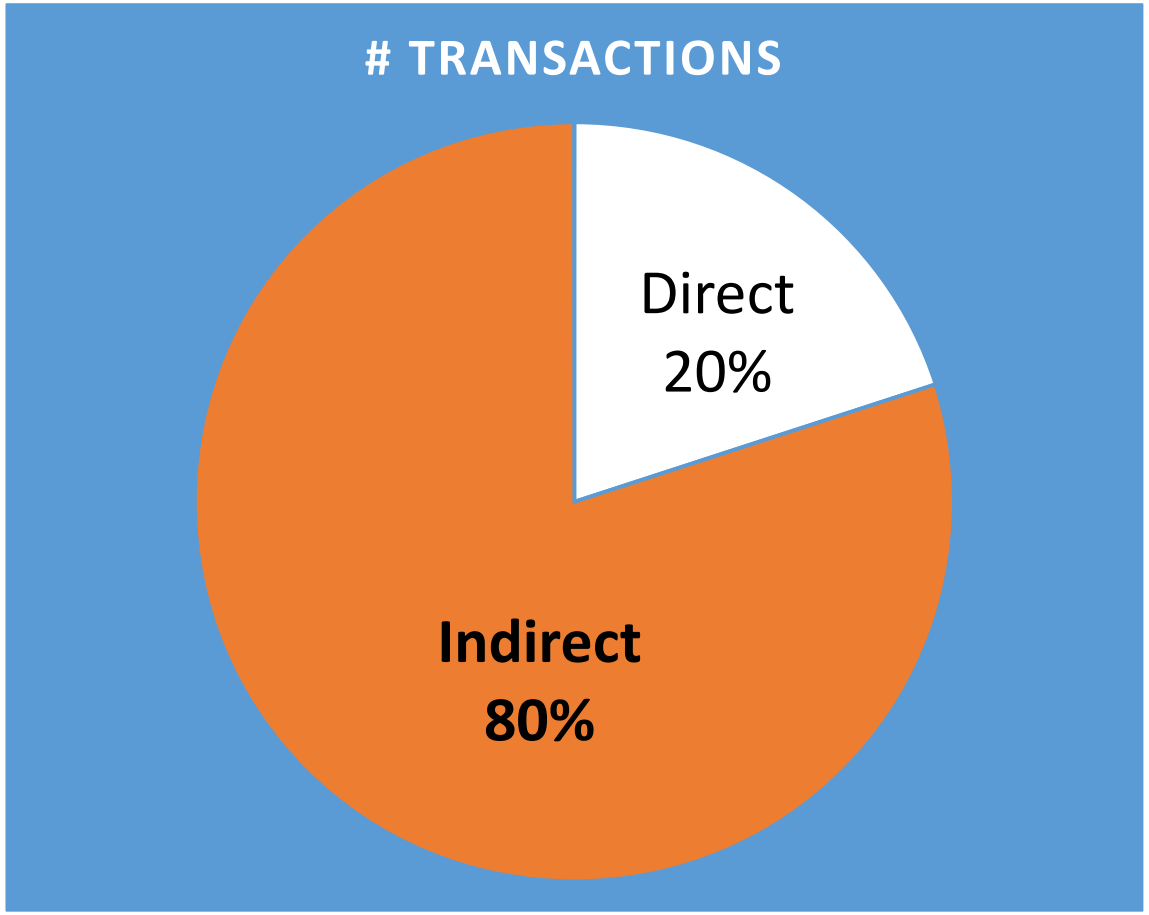
- Introduction - My Background
- Purchasing Card Program – fit into overall procurement strategy
- Purchasing Card Risk & Red Flags
- Internal Control & Governance
  - Preventive
  - Detective
  - Data Analytics
- Reporting & Communications
- Wrap up, Questions & Answers

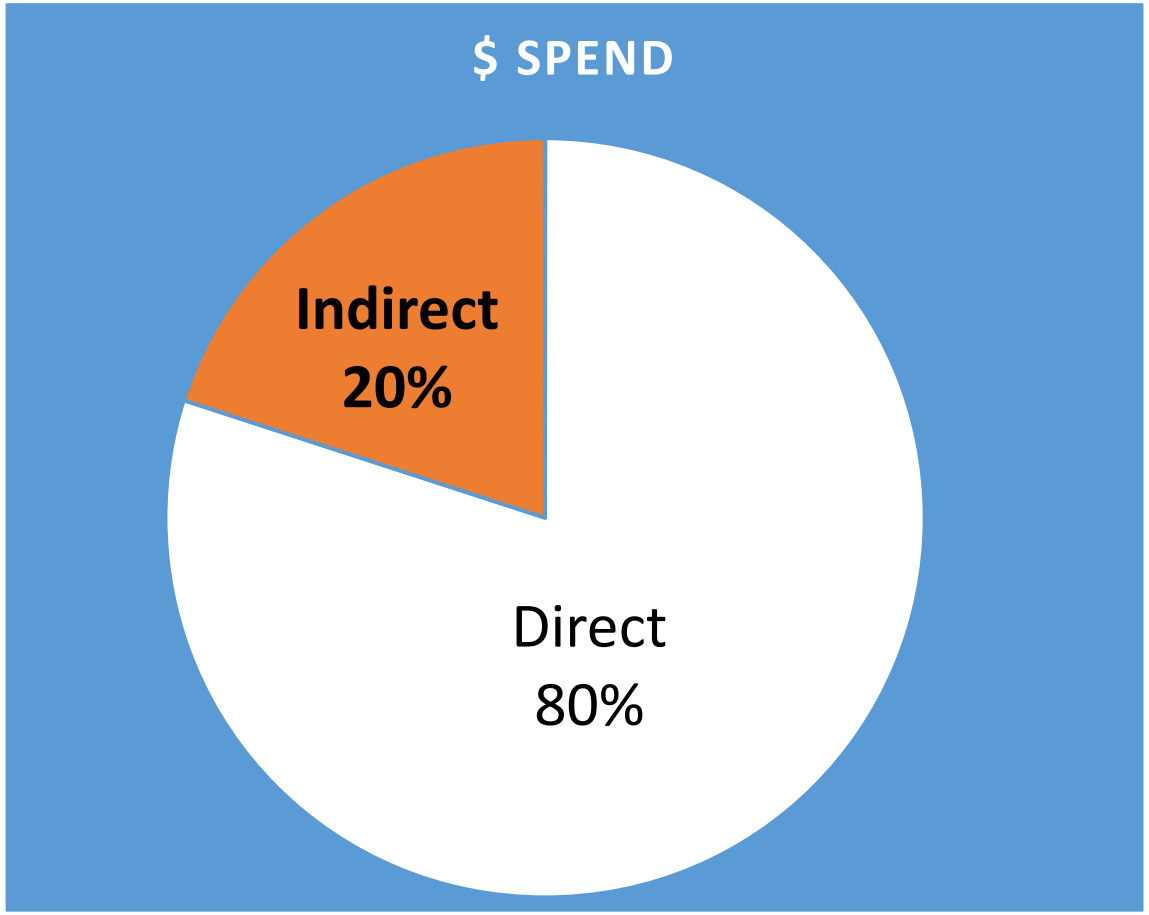
Background

- 17 years, Consulting, Risk Advisory & Internal Audit professional practice
- Big 4 Advisory (KPMG), BDO Seidman - across industries, incl. HE, NP
- Prior, Accounting & Finance positions in industry
- Now, independent practice, (Triplet Advisory Services) and partner with peer Consulting & RA firms
- Significant involvement with Purchasing Card programs, Supply Chain and Purchase to Payment process
- Held role as interim Purchasing Director

Where Purchasing Card fits?

Indirect spend – most of an organization's purchase transactions





P Card Program Fit

- Part of an overall supply chain management strategy
- Complementary to other purchasing & payment tools
- Purchasing & settlement strategy is segmented:
  - Purchase orders
  - E-procurement (catalogue)
  - Direct pays (no PO)
  - **Purchasing cards**
  - Petty cash
  - Checks
  - ACH
  - Wire transfers
  - E-payables (EAP)
- What spend and suppliers and are you targeting for card, vs. contract/PO, vs E-procurement, etc.?

Purchasing Commodity Strategy – matrix

Commodity	Designated Purchase Method	Secondary Purchase Method
Office Supplies	P-Card (ghost)	NA
Catering	P-Card	Direct pay
Industrial – sm. parts, tools, etc. (MRO)	E-Procurement (vendor site, e-commerce platform (Ariba) - PO	P- Card
Industrial – consumables, supplies (MRO)	P-Card	NA
Inventory	Purchase Order/EDI (contract)	NA
Equipment – under $5000	P- Card	Purchase Order
Equipment – over $5000 (capital)	Purchase Order	NA
Testing Services	Purchase Order	NA
Printing/Shipping	P- Card	Purchase Order

Card program goals must complement overall purchasing strategy

Risk Assessment

“Fraud is the dysentery of crime; even after the infection is contained, the unpleasant after-effects linger interminably”

- Jed Rakoff – Federal Judge NY District

Risk is Neutral Term

- Risk both poses threats and presents opportunities!
- Downside
  - Increased fraud
  - Lost funds, time consumed, investigation, litigation
  - **Reputation harmed**
- Upside
  - Cost savings & processing efficiencies in Purchasing & AP Depts.
  - Internal customer satisfaction
  - Revenues from earned rebate
  - Cost reductions obtained from suppliers through volume leverage
  - **Shift resources to critical, strategic, supply chain management for the business!**

Risk Appetite

- How much risk are you willing to accept to achieve your business objectives from program?
- Risk tolerance influences your internal controls in place.
- Companies have to take risk to make a profit, deliver value
- They may be able to tolerate, or absorb, a different level of risk without impact to achieving strategic objectives
- Reputation risk must always be managed!

Types of Risk

- **Program – Life Cycle**
  - Spend levels, cost savings, process efficiencies, revenue rebates
- **Internal**
  - Employee fraud
  - Purchasing policy compliance (misuse)
  - Company credit limit, late payment or average transaction size penalties
- **External** – Cybercrime, mobile technology, scamming, phishing, identity theft, email, fax, etc.

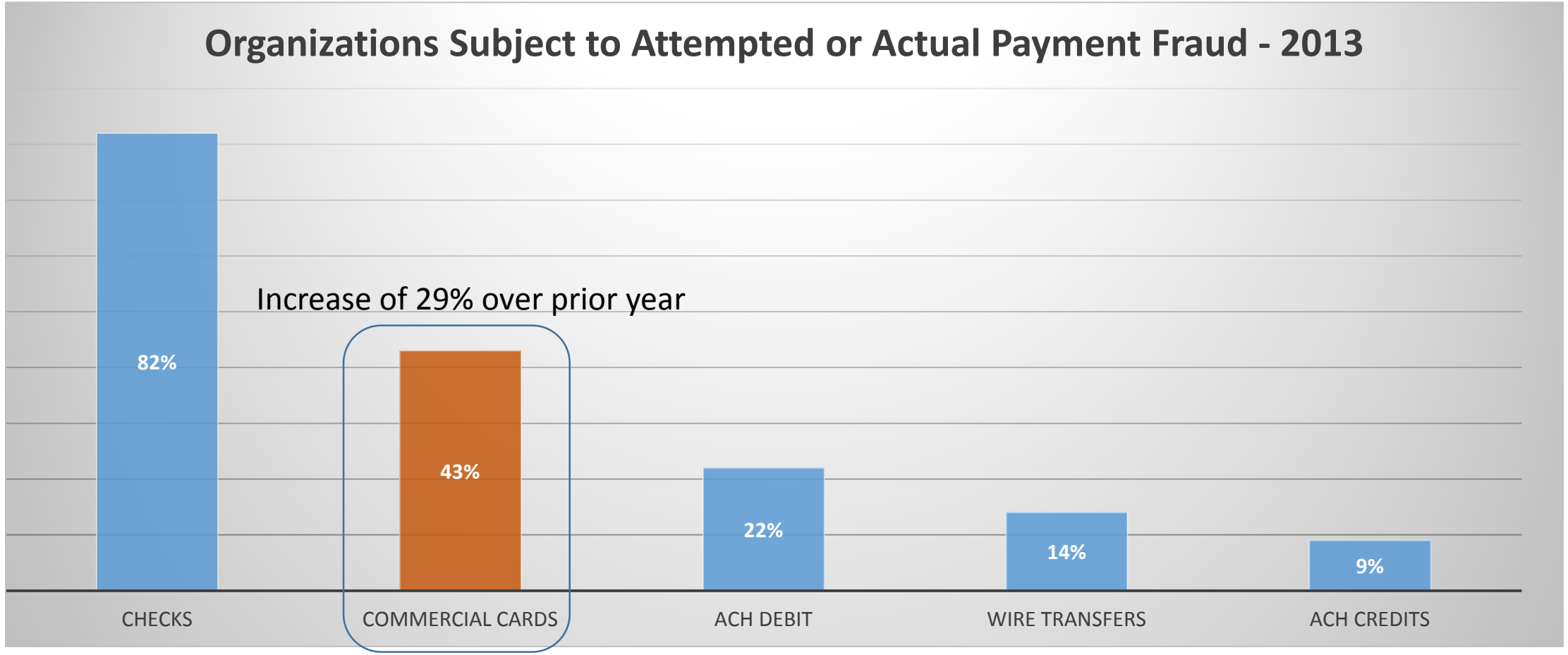
Program Life Cycle Risk

- Planning?
  - Assessing need, RFP, Evaluating card providers,? – **Choose right provider!**
- Deploying?
  - Are you piloting? – **Design, timeliness, adoption – initial wins & momentum!**
- Young – first few years?
  - Growth - **Employee & Vendor acceptance!**
- Mature?
  - Sustainability - **Usage**
  - Growth volume – **Targeting other spend categories?**
  - Expansion users - **More/new depts./business units/locations?**
  - Competitiveness – **Rebid?**

Risk – Different for types of business

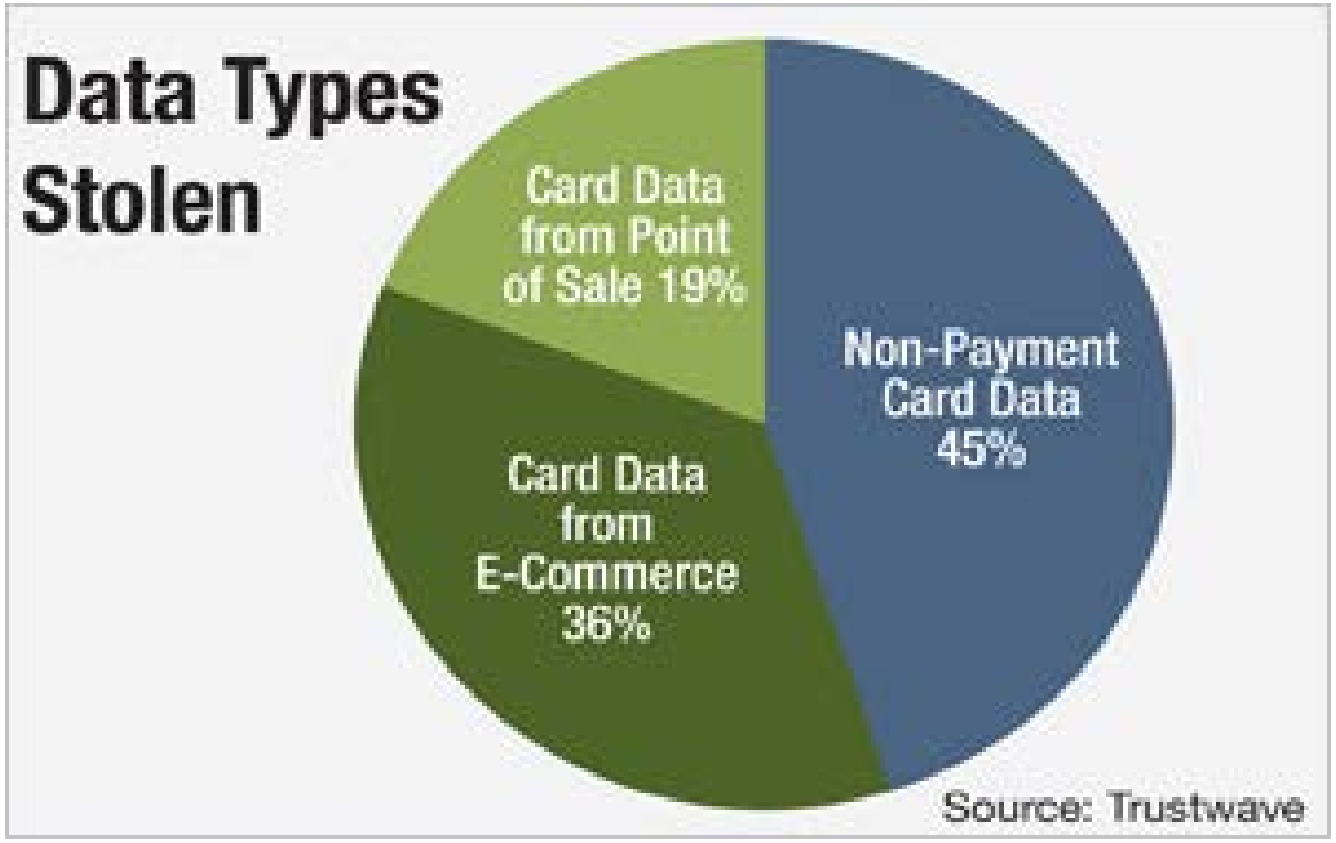
- A Washington Post analysis of filings from 2008 to 2012 found that more than 1,000 **nonprofit** organizations that checked the box indicating that they had discovered a **“significant diversion”** of assets, disclosing losses attributed to theft … and other unauthorized uses of funds. (Including misuse of credit cards)
- Higher inherent levels of trust
- Gaps in fraud awareness, control consciousness & even tech savvy
- Segregation of Duties (resources/practices); resource constrained
- Difference audit mentality - culture

Payment Fraud Trends



Source: Association for Financial Professionals (AFP)

Data Theft

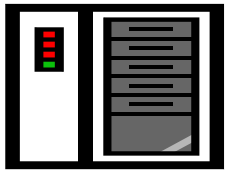


Non-Payment Card Data can be used to steal identity and card data!

Purchasing Card Ecosystem

Acquirers

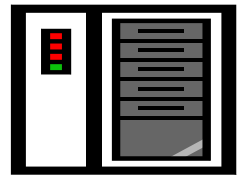
Issuers



Merchant Processors

Several points in payment system for potential data leakage!

Card Processors



Partners, Suppliers

Merchants/ Vendors

Cardholders

Card Purchases

Point of Sales (POS) system
On-Line Shopping Cart
Phone

Purchasing Card Fraud

- Despite attention getting news stories, the actual fraud impact overall historically is extremely low!
- 70% of companies exposed to actual or attempted fraud last year, experienced no financial loss as a result.
- Insurance and liability provided by Card issuers (banks) limit loss
- **HOWEVER, Image and reputation** can suffer enormously, especially if public funds are involved!
- Risk also a perceived internal barrier for card growth!

Source: Association for Financial Professionals (AFP)

Source of Fraud

- Commercial card fraud was most often perpetrated by an unknown **external** party, 57%
- Remember – fraudulent charges may not appear for months!
- Likely that small dollar charges will appear initially!
- Imperative for individual card holder and manager review
- DA (Data Analytics)

Source: Association for Financial Professionals (AFP)

Risk Events & Implications

- Physical cards with magnetic strips – easily counterfeited! (EMV coming)
- Businesses & organizations are “Extended Enterprises”
- Your exposure is widespread – merchants/suppliers, partners/vendors of suppliers, point of sale systems, payment processors, computers, tablets, mobile devices, smart phones, etc.
- **External (Cybercrime):** JP Morgan, Home Depot, Target, Kmart, SuperValue, Michael’s Stores, Goodwill Industries, UPS Stores, PF Chang’s, Global Payments, Heartland Payment Systems (3rd Party Processors)
- Fraudsters are very patient in selling, testing and using stolen card data

CNP – Card Not Present

- No signature required. Predominant trend in B2B.
- Website – Shopping Carts
- Email
- Phone (mobile)
- Fax

Also, harder to establish proof of delivery of shipped goods by merchant – (no signature required) > fraudulent returns

Ecommerce Precautions

- Purchasing - Supplier Management
  - PCI compliant, encryption, store user data?
  - Privacy & data protection policies? What?
  - What are their data access practices with their 3rd party partners & suppliers?
- Card Holder
  - Legitimate vendor (Address, company reviews, BBB)
  - Authenticate websites (enter URL directly)
  - Secure sites (https, padlocks, privacy management services provider certification: TRUSTe, e.g.)

Risk Reduction – market trends

- Magnetic strips to EMV (“chip & pin”) cards
- Awareness by larger and public companies to better security practices to ensure protection: encryption, dual authentication, firewalls, PCI, {compliance & regulatory}
- Caution with 3rd party partners and their access needs
- Reputational risk awareness
- Apple Wallet (IPay) with new IPhone – tokenization (cardless, contactless)
- Cost to convert their POS and hardware to accept EMV – smaller companies likely to be slower adopters!

Understand your procurement environment to reduce risk

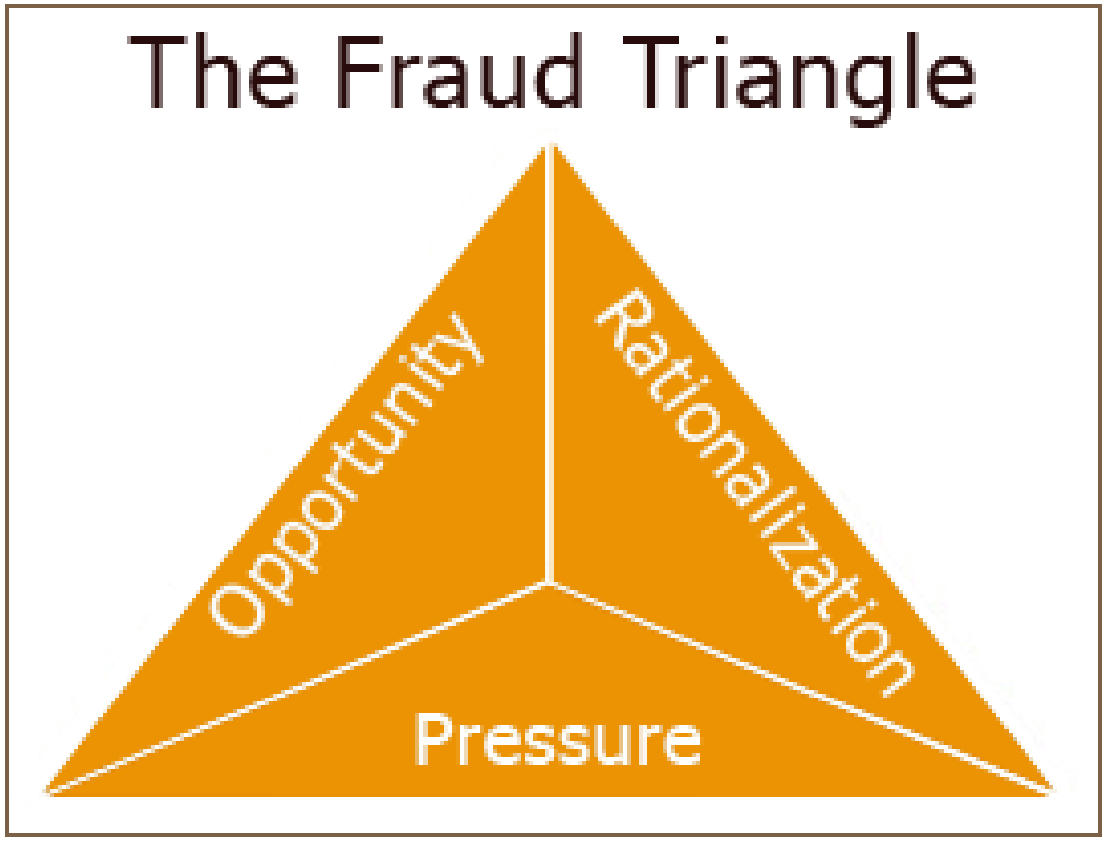
- What type of products/services are you buying (industrial/commercial vs retail)?
- Physical or online purchasing?
- Longtime, familiar suppliers or not?
- Local, national or international?
- **Can you trust your card user population to act responsibly?**
- **All employees** have a responsibility for risk management

Risk Summary

- P Card – highly efficient & cost effective procurement tool, but subject to risks that must be managed.
- Cost/benefit to an internal control implementation
- IC provides reasonable – not absolute assurance!
- Think holistically about the program.

Riskier Transactions

- New card holders
- High volume card users
- Users with history of declines – blocked transactions (merchant or $)
- Users that often spend up to their card limits
- Users with lost cards
- Unusual, unfamiliar vendors or addresses (e.g. PO Boxes)
- Recently terminated or LOA employee
- Unusual geographical use outside normal business area
- International (e.g. Nigeria, Mexico, India, Brazil, UAE, S. Korea, Eastern Europe, Russia)
- Split transactions
- Multiple purchases same vendor same/consecutive days
- Whole dollar amounts w/retailers
- **Wide span of control transactions for Mgr. review**


The Fraud Triangle
Opportunity
Rationalization
Pressure

D. Cressey

- Motive (or pressure) – the need for committing fraud (need for money, etc.)
- Rationalization – the mindset of the fraudster that justifies them to commit fraud
- Opportunity – the situation that enables fraud to occur (often when internal controls are weak or nonexistent).
- *Of the three elements, removal of Opportunity is most directly affected by the system of internal controls and generally provides the most actionable route to deterrence of fraud.*

Red Flags

- Almost all occupational fraud includes indication of certain behaviors:

Common personality traits:

- ***Lives beyond their means***
- Wheeler and dealer
- ***Domineering/controlling***
- Resists people reviewing their work
- Strong desire for personal gain
- Has a “beat the system” attitude
- Close relationship with vendors
- Unable to relax
- Often has a “too good to be true” work performance
- Doesn’t take vacation or sick time
- Often works excessive overtime
- ***Displays a drastic change in personality or behavior***

Purchasing Card Red Flags

- Late or no reconciliations
- No receipts or business justifications
- No manager review of transaction activity (including turnover)
- Gift card purchases
- ATM cash withdrawals
- Cash Advances

Internal Control & Governance

- Preventive
- Detective
- Entity Level
  - (tone at the top)

All are required!

Policies & Procedures (Soft)

- Careful card user selection, vetting & justification
- Approved application
- Card policies and user guide
  - Purchases matrix
- Mandated training (retraining)
- Signed cardholder agreement
- Sanctions, incl. termination
- Deterrence: Reinforce with cardholders that all transactions are monitored and subject to audit

Training

- No training – no card
- Up to organization to make sure employees understand safe purchasing practices – especially via internet!
- Verify vendor is legitimate and website is safe
- Never purchase via an email link
- Don’t store card info on vendor website
- Buy when in office – behind organization’s firewall as much as possible
- Never email/fax card information

Cardholder

- Limit card to a single user
- No card sharing within a department
- No department cards
- Cards secured at all times
- Receipts (scanned - incl. $ threshold)
- Process for cancelling terminated, transferred employee cards
- Assigning new Manager approvers
- Check transactions on-line - **frequently**

Spending

- Card spend limits
  - Transaction
  - Daily
  - Monthly
- Tailored by user or user profiles
  - Based on business need
- Limits shaped by spending analytics done earlier and risk tolerance
- Aligns with purchasing strategy and controls – should dovetail with Purchase Order and other spending control limits

Transaction

- Velocity or transactions per day
- No ATM use
- No cash advance use
- No Gift Card use

Supplier/Merchant

- Merchant commodity code blocking (MCC)
  - Type: e.g. casinos, liquor stores, strip clubs, massage parlors, etc.
  - Vendors/merchants outside normal geographical area
  - Unfamiliar or suspicious vendor names or addresses
- Supplier Block
  - Channel business to preferred supplier

Other Preventive Controls

- Background checks (HR)
- Segregation of Duties
  - Program Administrator (PA)
  - Cardholder/approver
- Recalibrate spend limits to history and needed limits
- Review/cancel - inactive cards
- Performance issues – probation
  - Inactivate cards
- Promptly restore 1X spend limit changes if made (PA)

Detective

- User statement reconciliation with business justification
- Manager review and approval of statement
- Manager monitors transactions **frequently**

- Purchasing Card Administrator review of transactions
  - Spot/ad-hoc audits or rotational
  - Anomalies - investigation
- Leverage fraud monitoring capabilities of card provider – have advanced monitoring in place. Make use of alerts.
- Internal Auditor –review

Detective – Trust but Verify!

- Numerous incidents of fraud committed by top management
  - No review process!
- **Controller or Board Chair reviews Senior Executive purchasing card statement**
- Controls apply to everyone in the organization!

Program Administrator

- Critical Role!
- Key person in influencing, configuring, and evolving your card program
- Must be responsible, principled, risk aware, control conscious, facility with data and trend analysis
- Good communicator!
- Have stature and respect within the organization
- **Able & willing to surface anomalies with users, management & IA**
- Gets to root cause, resolution, and necessary program changes

Data Analytics

- Continuous **monitoring** by program/ops management, or continuous **auditing** by independent IA function – policy compliance & controls assurance
- 100% Transaction Review against assigned higher risk criteria – “rules based”
- Runs near real time vs. delayed, manual transaction review
- Bank provider software platform – tools, reports, queries, or DA vendor
- Can have case management, escalation & resolution capabilities
- DA vendor software can incorporate scripts against other databases for enhanced control and detection (e.g. HR – employees, T&E system)

Data Analytics (DA)

Benefits:

- Enhance visibility and control – 100% population vs. random sample
- Improves compliance – P Card and purchasing policy
- Streamline back end monitoring & auditing– automates!
- Reduced cost to audit (vs manually)
- Flags high risk transactions consistently
- **Can serve as a strong deterrent!**

Why you need to monitor? Example!

- A State Government official used the card belonging to someone under him and purchased TV's, movies, cameras, electronic games, mobile devices, rental vehicles, hotel rooms, fuel, vacuum cleaners and dishwasher.
- Appeared goods being sold for large sums of cash.
- Theft went undiscovered for 4 years!
- The individual was Director of Auditing & Compliance in a State Agency!!!

Lessons Learned

- Can never be too trusting of anyone!
- Opportunity to commit can be high– remember the fraud triangle
- Polices and training won’t stop a determined fraudster
- Preventive controls can be circumvented
- Fraud can go undetected for years if not actively monitored

Trust - but Verify!

Data Analytics - criteria

- SOD – same person cardholder and approver
- Large span of control – more than X cardholders/txns. to an approver
- Active cards for terminated employees
- > X transactions or 80% of spend with same vendor
- Keyword searches
- Weekend, Evening & Holiday use
- Statement review & approvals
  - Not done/late
- Accounts > 1 lost/stolen card last 12 months
- Higher than average number of transactions last X cycles
- Inactive – no activity for X months
- Underutilized credit limits – avg. trend

Data Analytics

- Unauthorized MCC
- Split transaction/single card
- Split transaction/multiple cards
- Large spend increase vs. avg.
- Cash withdrawals
- Ship to other than company
  - EE Home Address
- Temporary increases > $ limit
- Multiple cards – same user
- Duplicate transactions –same merchant
- Duplicate payments: w/AP & T&E
- Fuel purchases
- Cardholder/merchant match
- Banned merchants (OFAC)
- Case management of violations & suspected fraudulent transactions
- Summary of spend by vendor
- Non-Preferred merchant

Governance, Entity Level – "Tone at the Top"

- Whistleblower policy & mechanism (hotline)
  - Anonymous , non-retaliatory & independent
- Code of ethics, anti-fraud, and conflict of interest policies
- Fraud awareness training, behavioral red flags and options for reporting fraud
- Background and credit checks
- Management reviews of (card) program reporting

Organizations lacking these controls experienced a 45% higher median loss! (ACFE)

Frauds are much more likely to be detected by **tips** than by any other method!

- *Organizations with some form of **hotline** in place saw a much higher likelihood that a fraud would be detected by a tip than organizations without such a hotline. (ACFE)*

Wise Perspective

"Somebody is doing something today ... that you and I would be unhappy about if we knew of it. That's inevitable: ... the chances of ... getting through the day without any bad behavior occurring is nil. ***But we can have a huge effect in minimizing such activities by jumping on anything immediately when there is the slightest odor of impropriety***. Your attitude on such matters, expressed by behavior as well as words, will be the most important factor in how the culture of your business develops. ***Culture, more than rule books, determines how an organization behaves"***

- Warren Buffett

Reporting Best Practices

- Dashboard format
- Calibrated to proper level (top management vs. BU. e.g.)
- Relate back to program goals established
- Includes Trending/Variances
- Strategic Purchasing metrics influenced by the card program
  - Competitive bids, RFP's, contracts, design-in, quality, delivery, cost savings **– and supplier performance management to meet organizational objectives**

Underlying Reporting Principles

- KPI's
  - Monthly or quarterly
  - Total, Business Unit, Dept.
  - Detail tiered to organization reporting structure
  - **Data for performance and that can be acted upon**
- Program Goals
  - $ spend, # cards, $ revenue (rebate)
- Exceptions - number/$
  - Investigated
  - Fraudulent
  - Write-offs

Other metrics

- Average $ spend/card
- Average $ transaction size
- Average # transactions/card
- # active/inactive cards
- # of declines
- Transactions/$ detail of transactions for investigation
- Ratio of cardholders to approvers*
- Average number of transactions reviewed per approver*

Other Metrics - Purchasing

- Top P card vendors
- Top P card users
- PO or other vehicle with these vendors (non-compliant)
- % of purchases under designated card $ threshold (opportunity)
- Savings achieved
  - $ Pricing actions (PPV) via leverage

Other Metrics – Purchasing/AP

- Average $ Spend/Supplier
- # of purchase orders placed
- # of invoices processed
- # of checks cut
- # active vendors – Vendor Master (consolidation) trend

Why do we need compliance?

"... The central mission of compliance needs to be maintaining and developing a well-founded and enduring business."

- Global Fraud Report , Kroll Advisory Unit

Wrap Up

- The payment landscape - ripe with opportunities for fraud and misuse
- Fraud is a “cat & mouse” game – constantly evolving with technology
- Fraudsters always looking to find the weakest link for data theft
- No system is fool proof!
- The human component for fraud – fraud triangle always present
- As program volumes ramp, the **oversight** function becomes diluted
- Data analytics has critically important monitoring role to play!

Wrap Up

- Card programs aren’t static! Must monitor risks!
- Up to card program management, operations, finance and internal audit to tweak the program based on your own history, risks, tolerances and needs
- But, don’t overly constrict the program - over arching business goals at stake!

“Trust, but Verify!”

Questions & Thank You

- Also, feel free to contact me or ask questions at:

Alan J. Goldberg, CIA, CRMA, MBA
Triplet Advisory Services
alan@tripletadvisoryservices.com
508.878.5570
http://www.tripletadvisoryservices.com
Twitter: @alan.j.goldberg