Account Fraud Prevention & Internal Controls

UNT UNIVERSITY OF NORTH TEXAS
Patrick Shinkle
University of North Texas
Center for Public Management
https://cpm.hps.unt.edu/

Objectives of this Session

- Understand the issues of account fraud
- Discuss the banking tools to assist detection
- Review examples of required verification for authentication
- Discuss recommended internal controls & depository controls
- Review methods to detect accounts payable fraud
- Discuss accounts payable "Red Flags"
- Discuss Ransomware Prevention
- Discuss structure and analysis of Benford's Law

Background:

- Protecting public funds is a high priority for all governments.
- The Uniform Commercial Code (UCC) regulates and defines the responsibilities of counterparties in business and banking transactions.
  - The UCC states that, in certain situations, liability and monetary loss in a fraudulent transaction is split between the counterparties in a transaction based on each party's due diligence and negligence. Consequently, to reduce liability in the event of a fraudulent transaction, it is important to have proper controls in place.

http://www.gfoa.org/bank-account-fraud-prevention

Email Scams – "Whaling Scam"

- Scam artists will use a similar "spoofed" email address to the one used by the entity or an individual at the entity.
- Typically asking for a wire transfer with specific nonstandard instructions.
- The message might include:
  - Knowledge of bypassing procedures
  - Personal conversation in nature or favor
  - Rush transaction
  - Fake situation
  - Emergency request
  - A link to a "familiar" website with possible login requirements
- The scam is also used to release confidential or sensitive data.

Banking Tools

- **Positive Pay:**
  - Bank compares checks that it receives for payment against the record of the checks issued by the government.
    - If the bank receives a check that does not match the information (date, check number, and amount) in the government's record, it identifies it as an exception item (i.e., a non-conforming positive pay item).
- **Payee Positive Pay**
  - Payee positive pay is an enhanced positive pay service that requires the validation of the payee name in addition to validating the date, check number, and amount.
- **Reverse Positive Pay**
  - Entity retains the record of checks issued and confirms with the bank before payment. Liability remains with the entity.

http://www.gfoa.org/bank-account-fraud-prevention

Banking Tools

- **ACH Blocks & Filters:**
  - Stop any attempt by an outside entity to process an ACH transfer and remove funds from a checking account without prior permission.
  - ACH blocks prevent all disbursements from an account.
  - ACH filters prevent disbursements that do not match a list of pre-authorized transactions or identification numbers. ACH filters involve:
    - (a) giving prior permission to certain approved business partners to draw upon the account,
    - (b) establishing an approval process for pending ACH transmissions, and/or
    - (c) setting maximum dollar limits on ACH debit transactions.
- **Limitations on International Transfers**

http://www.gfoa.org/bank-account-fraud-prevention

Banking Tools

- **Reconciliation tools:**
  - Allow governments to extract information/data from their bank or have information sent from their bank that assists the government in performing period end reconciliation of bank accounts.
  - The bank may also provide a tool that completes a full reconciliation of the account and produces detailed reports of reconciled items.
- **Universal Payment Identification Codes (UPIC):**
  - May be used instead of the government's bank account numbers so that the government's account numbers are not disclosed.
    - UPICs mask confidential banking information, reducing the risk of fraud while facilitating secure electronic payments.
    - UPICs are restricted to credit payments, preventing unauthorized debits.
    - UPICs remain with the customer regardless of banking relationships, making any change of bank or account transparent to trading partners.
    - UPICs point to a single bank account. However, one account can have several UPICs

http://www.gfoa.org/bank-account-fraud-prevention

Banking Tools

- **Intra-Day Access:**
  - Allows a government to see bank account transactions and activity that occur at various times throughout the business day.
  - The information may be accessed via online systems provided by the bank, as well as through other methods including fax, email, and direct transmission of data from the bank to the government's computer systems.

http://www.gfoa.org/bank-account-fraud-prevention

Example Procedures & Sample Form

1. Procedures for Processing Outgoing Wire Transfer
2. Request to Change Banking Information
3. Sample: Accounts Payable Electronic Payment Request Information Form (ACH)

Example 1: Processing Outgoing Wire Transfer

- When a wire request is received, the staff in receipt of the request will verify the request ***independently*** from the original request.
- The verification may be completed by using the following information:
  - Email/telephone listed in vendor/requestor file – do not respond to email or telephone listed in/on the original request.
  - If the vendor file does not list an email or phone number, go to the company website and locate the contact information or use an invoice that was successfully processed prior to the current request.
    - Do not use any links provided in the original request.
  - If contact information cannot be obtained/verified through the above methods, a letter confirming the wire request will be sent to the main vendor address and out-going wire request will not be processed until verification is received from the requestor.

Example 1: Processing Outgoing Wire Transfer

- Once the validity of the wire request is verified, the date, time, method of verification and the name of the person contacted at the company/employee will be noted on the original request which may be the invoice, and/or journal entry supporting documentation. The staff who verified information will sign the original request.
- The original request / invoice will then be given to the Accounting Manager, or an Accountant to sign off that the request was verified to be initiated via bank portal.
- The **verified** wire request will then be processed by authorized accounting staff via City's bank portal that is set up with a 2 step approval.
- The bank portal wire confirmation must be attached as supporting documentation to invoice and/or journal entry and verified with the receiver of the wired funds.
- Processing employees sign the procedure document.

City of San Marcos: Operational Procedures

Example 2: Request to Change Banking Information

- All requests to change banking information (Accounts Payable / Payroll) must be verified with the requesting party ***independently*** from the original request.
- The verification may be completed by using the following information (Accounts Payable):
  - Email listed in vendor file-do not respond to original email that included the request.
  - Telephone number listed in vendor file-do not call the telephone listed on/in the request.
  - If vendor file does not list an email or phone number, go to company website and locate the contact information or use an invoice that was successfully processed prior to the request. Do not use any links provided in the original request.
  - If contact information cannot be obtained through the above methods, a letter confirming the change will be sent to the main vendor address and banking information will not be changed until verification is received from the requesting company.

City of San Marcos: Operational Procedures

Example 2: Request to Change Banking Information

- The verification may be completed by using the following information (Payroll):
  - Employee's City email-do not respond to the original email that included the request.
  - Employee's City extension
- Once the validity of the change is verified, the date, time, method of verification and the name of the person contacted at the company/employee will be listed on the request form and the verifier will sign the form.
- The request form will then be given to the Accounting Manager, or an Accountant in the Accounting Manager's absence, to sign off that the request was verified and the change is approved.
- The approved request form will be given to the Finance administrative assistant, who will make the change to the vendor set up in the system.
- Once the change is made, the verified request form will be attached to the vendor record in the system.
- Processing employees sign the procedure document.

City of San Marcos: Operational Procedures

3. Sample AP ACH Form

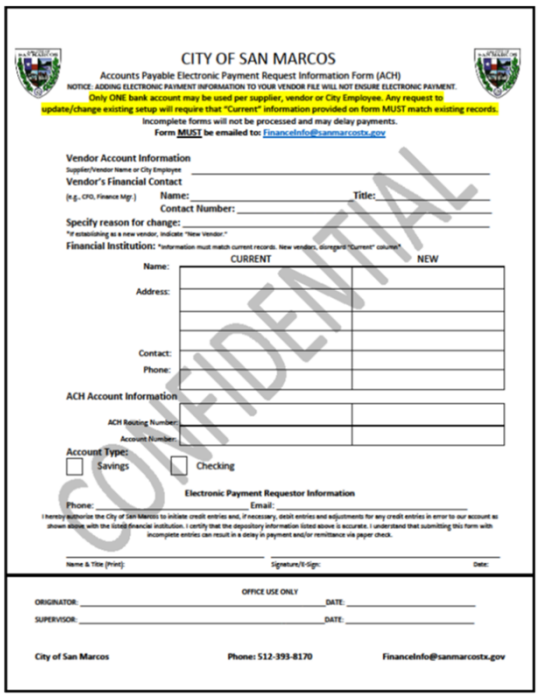
AP Electronic Payment Request Info. Form (ACH)

NOTICE: ADDING ELECTRONIC PAYMENT INFORMATION TO YOUR VENDOR FILE WILL NOT ENSURE ELECTRONIC PAYMENT.

Only ONE bank account may be used per supplier, vendor or City Employee. Any request to update/change existing setup will require that "Current" information provided on form MUST match existing records.

Incomplete forms will not be processed and may delay payments.

Form MUST be emailed to:
FinanceInfo@sanmarcostx.gov



CITY OF SAN MARCOS

Accounts Payable Electronic Payment Request Information Form (ACH)

NOTICE: ADDING ELECTRONIC PAYMENT INFORMATION TO YOUR VENDOR FILE WILL NOT ENSURE ELECTRONIC PAYMENT.

Only ONE bank account may be used per supplier, vendor or City Employee. Any request to update/change existing setup will require that "Current" information provided on form MUST match existing records.

Incomplete forms will not be processed and may delay payments.

Form MUST be emailed to: FinanceInfo@sanmarcostx.gov

Vendor Account Information

Supplier/Vendor Name or City Employee

Vendor's Financial Contact

(e.g., CFO, Finance Mgr.) Name: Title:

Contact Number:

Specify reason for change:

"If establishing as a new vendor, indicate "New Vendor."

Financial Institution: *information must match current records. New vendors, disregard "Current" column*

	CURRENT	NEW
Name:		
Address:		
Contact:		
Phone:		

ACH Account Information

ACH Routing Number:		
Account Number:		

Account Type: ☐ Savings ☐ Checking

Electronic Payment Requestor Information

Phone: Email:

I hereby authorize the City of San Marcos to initiate credit entries and, if necessary, debit entries and adjustments for any credit entries in error to our account as shown above with the listed financial institution. I certify that the depository information listed above is accurate. I understand that submitting this form with incomplete entries can result in a delay in payment and/or remittance via paper check.

Name & Title (Print): Signature/E-Sign: Date:

OFFICE USE ONLY

ORIGINATOR: DATE:

SUPERVISOR: DATE:

City of San Marcos Phone: 512-393-8170 FinanceInfo@sanmarcostx.gov

CONFIDENTIAL

City of San Marcos: Operational Procedures

Recommended Internal Controls

- Conduct periodic surprise audits and annual reviews of procedures.
- Provide for the physical security of all checks.
  - Maintain check images in preference to paper copies.
  - Keep check stock in a locked and secure location with a formal inventory listing maintained.
    - Secure check stock daily.
    - Remove continuous check stock from printers.
    - Lock and secure check specific printers.
    - Consider the use of blank or unprinted check stock with inventory control numbers. The actual check number may be generated through the financial accounting system.

http://www.gfoa.org/bank-account-fraud-prevention

Recommended Internal Controls

- Provide for the physical security of all checks.
  - Physically void returned checks and check copies
  - Retain in a locked and secure location or destroy on a schedule.
  - Provide for the temporary physical security of electronically deposited checks, including:
    - Storage in a secure facility,
    - Timely destruction such as secure shredding. (The depositing government is liable for any fraudulent usage of these checks.)

http://www.gfoa.org/bank-account-fraud-prevention

Recommended Internal Controls

- Ensure appropriate security over signature plates, cards, and software.
- Require additional review process for all checks over a specified amount.
- Consider using a Controlled Disbursement account, to the extent permitted by law, for all payroll and Accounts Payable disbursements to provide additional control. It is preferable to make payments via batch ACH (direct deposit) for both Payroll and Accounts Payable as opposed to checks to reduce fraud potential and payment expenses.
- Require two party authorizations (initiation and release) on all wires and ACH files.
- Require daily staff reconciliation of wires and ACH releases.

http://www.gfoa.org/bank-account-fraud-prevention

Recommended Internal Controls

- Ensure proper segregation of duties among staff initiating, authorizing, preparing, signing, and mailing payments and reconciling bank statements.
- Review signature cards and authority levels whenever any changes occur and annually at a minimum. Remove individuals from bank transaction authority immediately upon resignation or termination.
- Review all bank accounts at least annually. Consolidate or eliminate bank accounts that are not frequently utilized.
- Depending on the complexity, size and volume, consider segregating cash inflow and outflow in separate accounts to allow for placement of appropriate fraud prevention practices and products. When appropriate (i.e. if no restrictions exist) these types of separate accounts should be maintained as Zero Balance Accounts (ZBAs) that are swept into the governmental entity's concentration account.

http://www.gfoa.org/bank-account-fraud-prevention

Recommended Internal Controls

- Ensure that controls exist for the storage and destruction of all documents that contain account and other related information.
- Determine that appropriate controls are present if employees access the government's financial and banking systems from remote sites (i.e., restrict the sharing of files).
- On at least an annual basis, request the government's legal counsel to research changes in laws that shift liability for fraudulent transactions to the government.

http://www.gfoa.org/bank-account-fraud-prevention

Depository Institution Controls Review

- Implement positive pay, or preferably payee positive pay, on all disbursement bank accounts and reconcile exceptions daily. Positive pay is the single best fraud prevention tool available. If a government's bank offers a positive pay service and the government chooses not to utilize it, then the government (not the bank) will be liable for fraudulent transactions.
  - Instruct the bank to return all non-conforming positive pay items as the default instruction.
  - Ensure that a clear policy exists to separate responsibilities between staff approving positive pay exceptions and staff initially requesting and/or preparing the check.
  - Avoid reverse positive pay because with this service the liability remains with the government.

http://www.gfoa.org/bank-account-fraud-prevention

Depository Institution Controls Review

- Direct the bank to reject or block any and all withdrawals not initiated by the government from accounts that only accept deposits.
- Place ACH filters and/or blocks on all accounts.
- Place total or selective ACH blocks on all disbursement accounts. Selective ACH blocks, also known as ACH filters, allow electronic debits to occur only for pre-designated transactions.
- Develop a formal plan to review ACH blocks/filters. This should be done on an annual basis, at a minimum.
- Consider the use of Universal Payments Identification Codes (UPIC) for all receivables accounts.

http://www.gfoa.org/bank-account-fraud-prevention

Depository Institution Controls Review

- Ensure that your financial institutions provides for multi-factor identification for on-line banking services involving transactions and administrative functions. Ensure separation of duties (initiation and release/approved) for financial transactions and administration of the on-line system. Multi-factor identification may include numerous passwords and/or utilization of user specific tokens.
- Ensure that your financial institution provides a quarterly listing, by account, of all approved signers and access-only individuals.
- Utilize bank reconciliation services to reduce time on reconciliation and focus on exception items.
- Discuss enhanced or new account security features with your financial institution on at least an annual basis.

http://www.gfoa.org/bank-account-fraud-prevention

10 ways to Identify Accounts Payable Fraud

- Duplicate Payments
  - Duplicate payments in most cases may not be fraud-related, but can be a significant A/P issue that is both preventable and recoverable.
- Benford's Law
  - A pattern of naturally occurring numbers that should be consistent across any set of "natural" numbers.
- Rounded Amount Invoices
  - Invoices with rounded amounts, which are invoices without pennies.
- Invoices Just Below Approval Amounts
  - Dollar thresholds for management approval
- Check Theft Search
  - Identify missing check numbers or gaps in reconciled checks numbers. This is usually indicated on the bank statement with a '*" or '#' to indicate the check number is not sequential.

https://www.auditnet.org

10 ways to Identify Accounts Payable Fraud

- Abnormal Invoice Volume Activity
  - Rapid invoice volume increases may indicate a legitimate increase in business, but also may indicate fraudulent activity.
- Vendors with Cancelled or Returned Checks
  - Many cancelled checks or a regular pattern of cancelled checks.
- Above Average Payments per Vendor
  - Invoices that are way above average for a particular vendor.
- Vendor / Employee Cross-Check
  - Compare your vendor file and employee file by the following variables:
    - Address, Tax ID Number, Phone Number, Bank Routing Number
- Vendors with a Mail Drop as an Address

https://www.auditnet.org

AP Fraud Red Flags

- Expedited or urgent instruction requests
- Untimely instruction changes
- Only electronic communications
- Poor documentation
- Deviation from protocol and/or procedures
- Unusual or unapproved Vendors
- Increased payments to particular vendors without corresponding increases in goods or services
- Very large payments to one vendor
- Unusually large purchases on an employee's company-issued credit card

https://i-sight.com/resources/accounts-payable-fraud/

AP Fraud Red Flags

- Payments that consistently fall just under the amount requiring authorization
- Invoices in numerical or accounting sequence
- Invoices that look unprofessional, photocopied or edited
- Invoices that are missing key details, such as address, phone number, authorizing information
- A vendor's email address that uses a free provider, such as Gmail
- Multiple invoices paid together or on the same date
- Vendor addresses that are the same as an employee address
- Vendor address that look to be residential addresses

https://i-sight.com/resources/accounts-payable-fraud/

AP Fraud Red Flags

- Vendors with similar names
- Large entertainment, gift or expense charges
- Rounded dollar amounts
- Incomplete documentation or copies instead of originals
- Duplicate payments to the same vendor
- Vendor's prices that seem unusually low or high
- Close relationships between an employee and vendor
- Repeated purchases from a vendor with a record of poor quality goods or services
- Tips or complaints from employees, customers or vendors

https://i-sight.com/resources/accounts-payable-fraud/

Ransomware Prevention

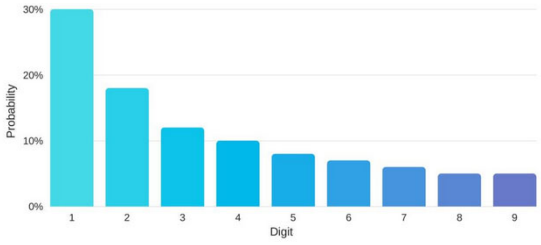
- Training and education of staff
- Strong policy development
- Strong antivirus and malware protection
- Effective backup and restoration procedures
- Restriction of users network permissions - Least privileges
- Enhanced email security
- Effective monitoring
- Review and testing of current security measures

Benford's Law

- Benford's Law is a great mathematical tool for screening accounts payable records for fraudulent payments.
- Benford's Law outlines a pattern of naturally occurring numbers that should be consistent across any set of "natural" numbers, such as payment records. When numbers are manually added into a naturally occurring set of numbers, they don't match the pattern dictated by Benford's Law.

Benford's Law

The principle that in any large, randomly produced set of natural numbers, such as tables of logarithms or corporate sales statistics, around 30 percent will begin with the digit 1, 18 percent with 2, and so on, with the smallest percentage beginning with 9. The law is applied in analyzing the validity of statistics and financial records.



d	$P(d)$	Relative size of $P(d)$
1	30.1%	
2	17.6%	
3	12.5%	
4	9.7%	
5	7.9%	
6	6.7%	
7	5.8%	
8	5.1%	
9	4.6%	

Benford's Law

- If a company has a rule that expenditures over a certain amount, say $1,000, require a second signature, an accounts payable employee writing fraudulent checks might keep the amounts below that threshold.
- In this case, a disproportionate number of checks might be written for amounts in the 900s, with a starting numeral of 9.
- Since the numeral 9 should occur naturally as the first digit only 4.6 per cent of the time, a lot of payments beginning with a 9 will throw the number set off the expected pattern.
- This is a red flag in an audit of accounts payable records.
- There may, of course, be a logical explanation for numbers not falling in line with Benford's Law, but it is an indicator that something is influencing the numbers and breaking the natural pattern.
- The fraud examiner then can investigate the cause of the anomaly to see if there is fraud occurring.

https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html

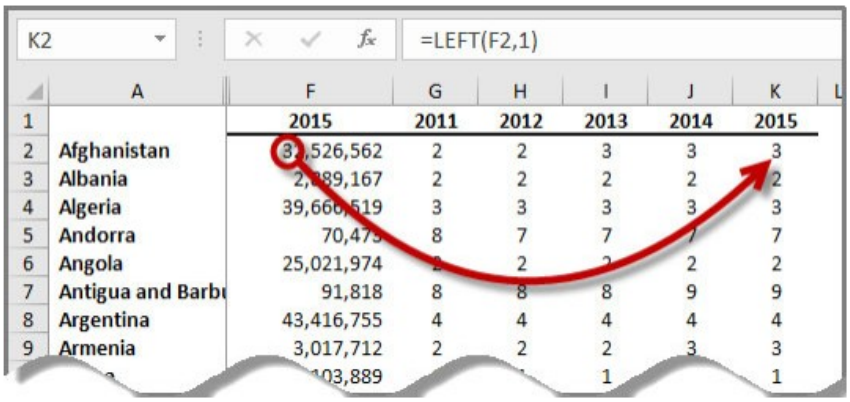
Benford's Law – Using Excel

- Simplified example using Excel. For this example, we will examine the populations of the world's 258 countries from 2011 through 2015 as reported by the World Bank Group's World DataBank
  - The first step is to extract the first digit of each population number using the LEFT function (see the screenshot "Extracting the First Digit"). As pictured in cell K2, the function formula =LEFT(F2,1) reads the population in cell F2 (32,526,562 in this example) and returns the first digit of that number (the digit 3 in this example).
  - This simple formula is then copied across and down to extract the first digits for all populations (columns G through K in this example).

https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html

Benford's Law – Using Excel

Extracting the first digit



	A	F	G	H	I	J	K
1		2015	2011	2012	2013	2014	2015
2	Afghanistan	3[illegible],526,562	2	2	3	3	3
3	Albania	2[illegible],889,167	2	2	2	2	2
4	Algeria	39,666,519	3	3	3	3	3
5	Andorra	70,47[illegible]	8	7	7	7	7
6	Angola	25,021,974	2	2	2	2	2
7	Antigua and Barbu	91,818	8	8	8	9	9
8	Argentina	43,416,755	4	4	4	4	4
9	Armenia	3,017,712	2	2	2	3	3
		[illegible]03,889			1		1

https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html

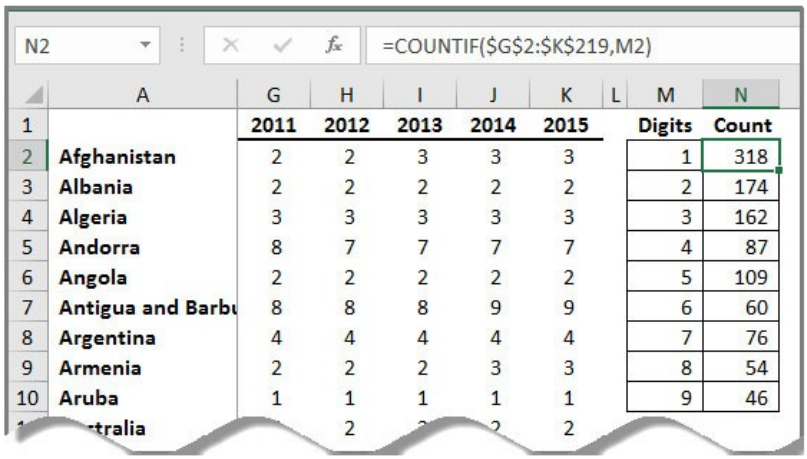
Benford's Law – Using Excel

- The next step is to count the occurrence of each number 1 through 9 within the extracted digits using the =COUNTIF function (see the screenshot "Applying the COUNTIF Function").
- This is achieved by numbering a range of cells 1 through 9 (as shown in cells M2 through M10), entering into cell N2 the formula =COUNTIF($G$2:$K$259,M2), and then copying that formula down to cell N10.

https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html

Benford's Law – Using Excel

Applying the COUNTIF function



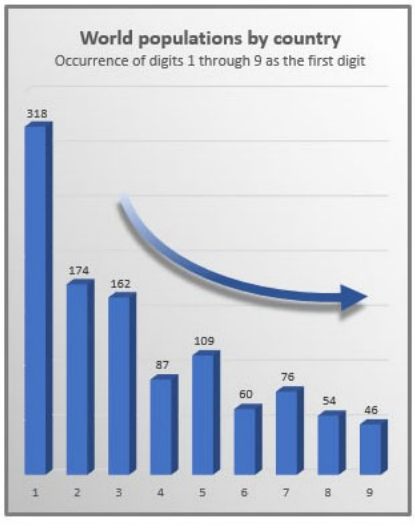
N2 =COUNTIF($G$2:$K$219,M2)

	A	G	H	I	J	K	M	N
1		2011	2012	2013	2014	2015	Digits	Count
2	Afghanistan	2	2	3	3	3	1	318
3	Albania	2	2	2	2	2	2	174
4	Algeria	3	3	3	3	3	3	162
5	Andorra	8	7	7	7	7	4	87
6	Angola	2	2	2	2	2	5	109
7	Antigua and Barbu	8	8	8	9	9	6	60
8	Argentina	4	4	4	4	4	7	76
9	Armenia	2	2	2	3	3	8	54
10	Aruba	1	1	1	1	1	9	46
	tralia		2			2		

https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html

Benford's Law – Using Excel

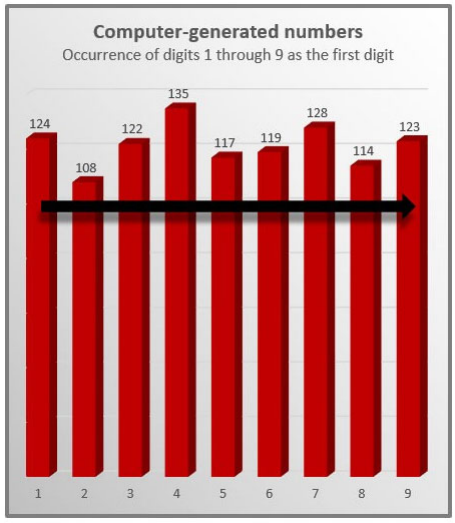
- As you can see in the chart, even with this relatively small data set, the results do roughly (but not exactly) follow Benford's curve. (While you should never expect the results to exactly match Benford's curve, you should expect the curve produced by larger sets of data to match Benford's curve more closely than in this relatively small data set example.)
- As a result, we can conclude that this Benford analysis tends to verify the populations as genuine numbers that have not been fabricated.



https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html

Benford's Law – Spotting Fraud

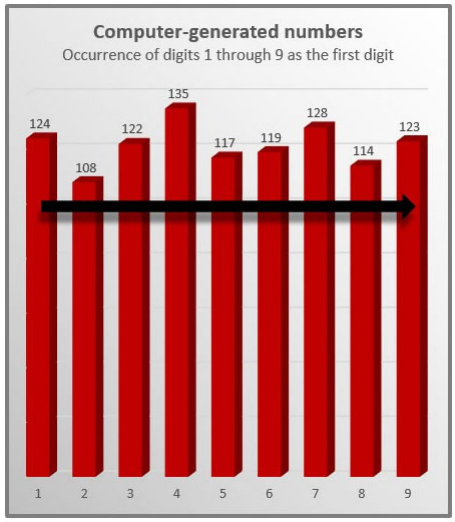
- To illustrate what a bar chart based on fraudulent or fabricated numbers might look like, I replaced the country population figures (from the earlier World DataBank example) with computer-generated random numbers by entering the formula =RAND()*10000 in place of each population number. The result is the chart "Computer-Generated Numbers."



https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html

Benford's Law – Spotting Fraud

- The top of the bars do not produce anything close to a Benford curve, and this straight-line result tends to repeat even when the random numbers are recalculated multiple times (by pressing the F9 key).
- This suggests these data were artificially produced, which they were using a standard computerized random number generator program, whereby each numeral 1 through 9 has an equal chance of being the leading digit.
- If the data you analyze produce a chart with bars of approximately the same height, this suggests the underlying data may be fabricated.



https://www.journalofaccountancy.com/issues/2017/apr/excel-and-benfords-law-to-detect-fraud.html