Session Number S22
Medical Identity Theft

The Health Plan Perspective

Tamara Neiman, Director, National Special Investigations Unit
Kaiser Permanente

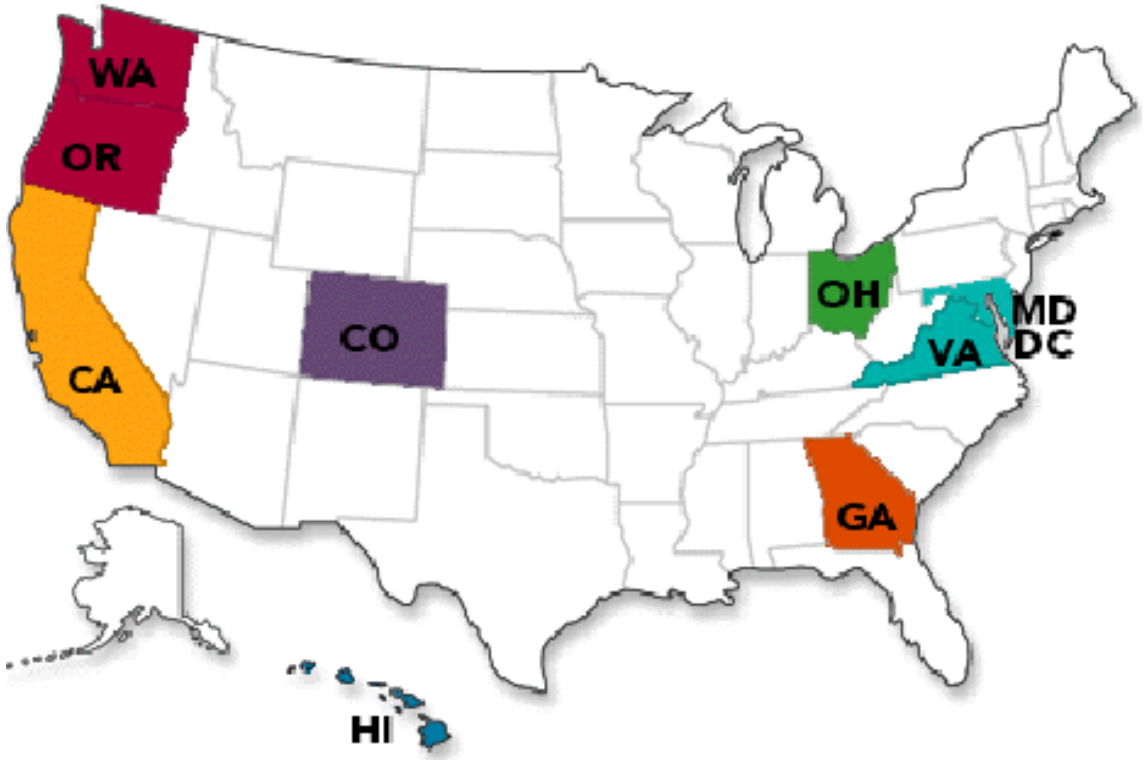
Jay Loden, Asst. Director, Data Analytics, Kaiser Permanente

Objectives

- Learn about Kaiser Permanente and its industry-leading electronic health record
- Learn medical identity fraud definitions and recognize the regulatory environment for medical identity fraud, related HIPAA violations
- Learn how Kaiser Permanente protects its members from medical identity fraud through proactive data mining and analysis
- Learn how to prevent and identify potential medical identity fraud through analytical data mining

About Kaiser Permanente

Founded in 1945, Kaiser Permanente is one of the nation's largest nonprofit health plans, serving close to 9.1 million members, with headquarters in Oakland, California.

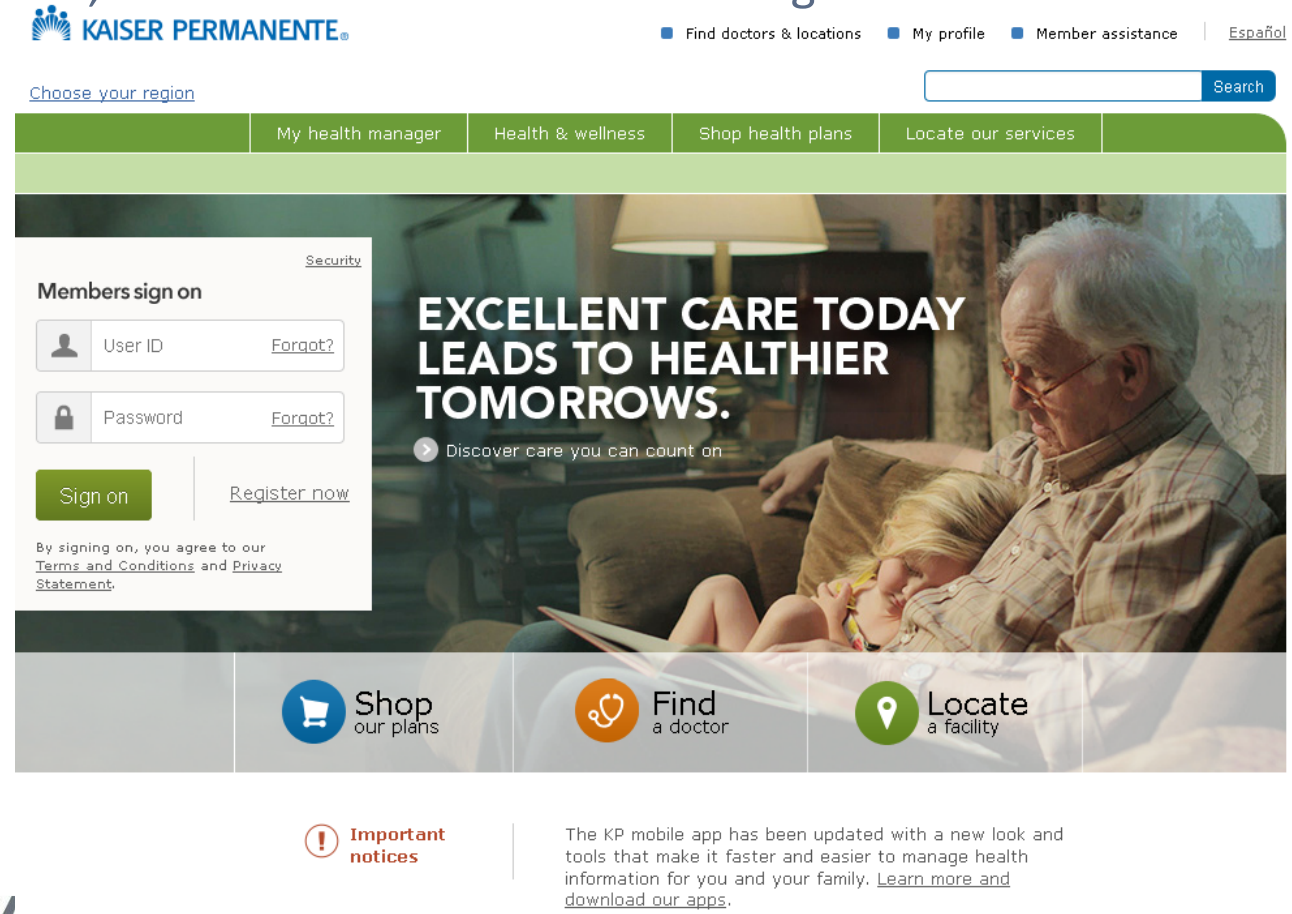


By the Numbers

Total Membership	**9,056,234 Million**
Hospitals	37
Medical offices	618
Physicians Approximate, representing all specialties	17,157
Nurses	49,034
Employees Approximate, representing technical, administrative, and clerical employees and caregivers (includes 45,270 nurses)	175,668
Doctor office visits (annually)	36.3 Million
Prescriptions filled (annually)	83 Million
Number of outpatient pharmacies	400
Operating Revenue	$50.6 Billion

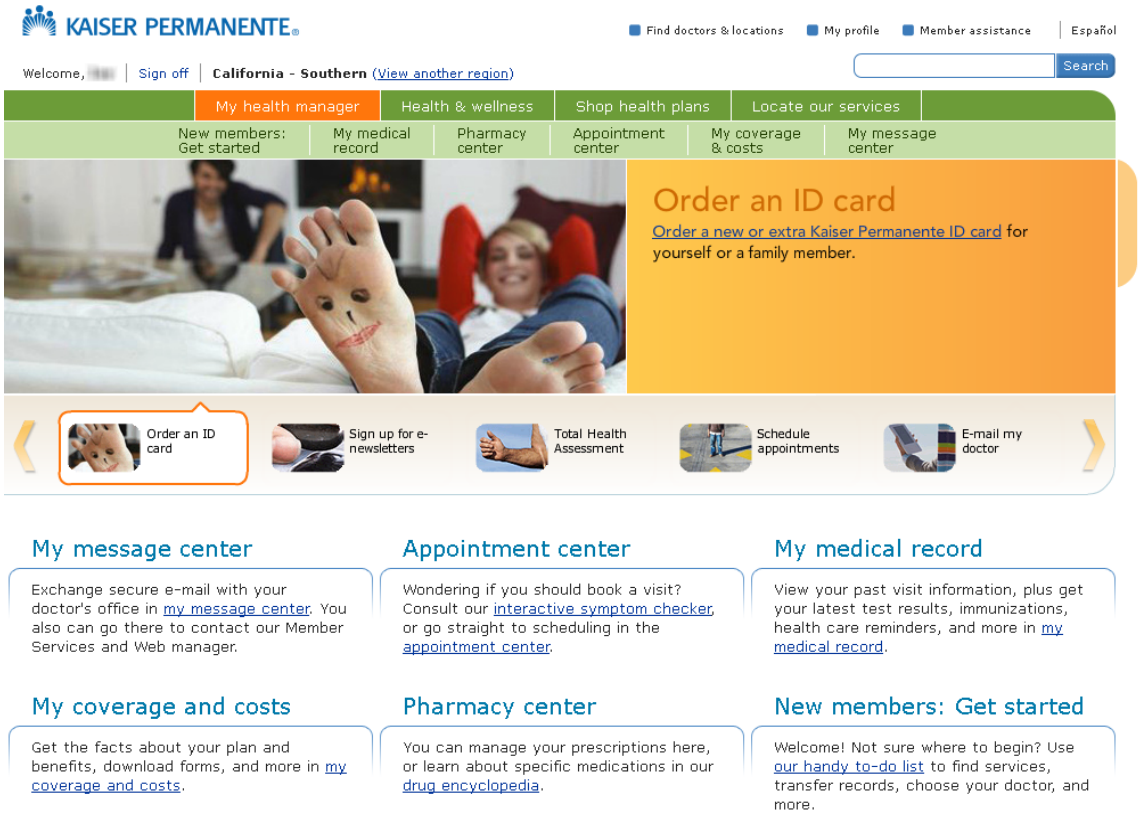
Industry-leading Personal Health Record

Kaiser Permanente HealthConnect® is an electronic health record (EHR), linking our 9.1 million members securely to their health care teams, personal health data, and the latest medical knowledge



My Health Manager on kp.org

- Kaiser Permanente HealthConnect® is the combination of our Electronic Medical Record (EMR) and Personal Health Record (PHR) (My Health Manager)
- In March 2010, every medical facility within Kaiser Permanente was equipped with HealthConnect EMR



Kaiser Permanente HealthConnect® by the Numbers

Secure signons to My Health Manager	88 Million
Secure emails (Sent to / from physicians and clinicians)	13.4 Million
Lab test results viewed online	32.3 Million
Visits to kp.org, averaging about 130,000 visits per day	116 Million
Online requests for appointments	3.2 Million
Online pre	Million

Medical Identity Fraud

- Medical identity fraud occurs when a patient's identity is used by someone else to get health care
  - An individual may be complicit in medical identity fraud by sharing his/her medical card with family or friends

    OR
  - Medical identity fraud can occur through other means such as when someone's wallet is stolen or patient data is sold to bogus vendors who falsely bill the government
- Criminal activity:
  - Identity theft
  - Theft of medical services
  - Medicare / Medi-Cal fraud (billing)

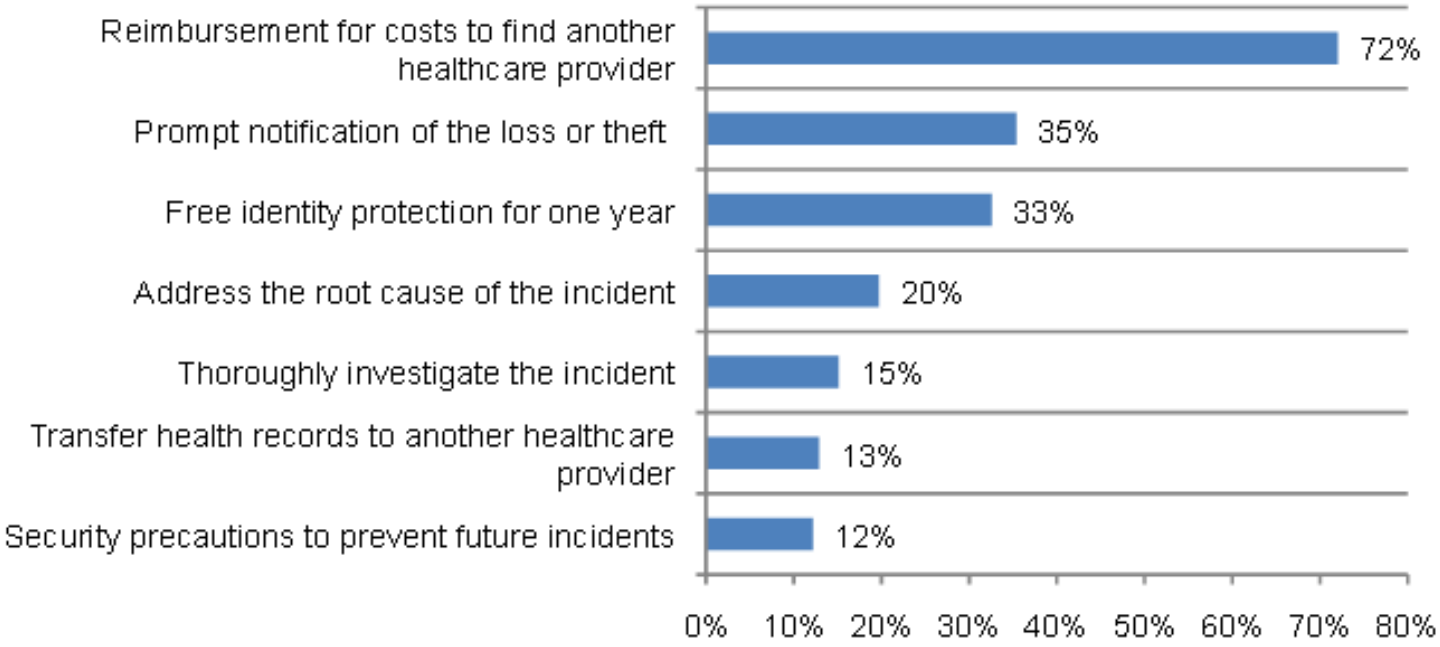
Risk Landscape

- Lost and stolen Protected Health Information (PHI)
  - Unencrypted devices of all types
  - Unintended disclosures
- Inappropriate access to PHI
- Health Insurance Exchanges (HIX)
  - They are here!
- Increased regulatory oversight
  - Greater fines and penalties

Risk Landscape

If notified that their medical records were lost or stolen, respondents would want the healthcare provider to reimburse them for what they paid to find another provider. Figure 2 reveals the top three actions desired by respondents following a medical identity theft. These are: reimbursement for costs to change to another healthcare provider, notification within 30 days of the loss or theft and free identity protection for one year.

Figure 2. Actions to be taken if notified that medical records were lost or stolen
Two choices permitted



Source: *Ponemon Institute© Research Report, Third Annual Survey on Medical Identity Theft*

Potential Consequences of Medical ID Fraud

- Compromised medical records that could create patient safety issues
  - Allergic reactions
  - Incorrect medical history
- False medical/pharmaceutical billings/claims
- Denial of health insurance claims
- Denial of health insurance coverage
- Denial of life insurance claims
- Denial of life insurance coverage
- Denial of employment based on false medical history
- Time and expense correcting false patient/insurance records

The Cost of ID Theft

Phony treatments: costly form of ID theft

Last year's economic stimulus bill includes $2 billion to create a national system of computerized health records, but one of the risks is more medical identity theft. Impersonating patients or setting up fake clinics to bill for phony treatments can be much more damaging than other types of identity theft.

Source: Javelin Strategy & Research, 2009 data

BLOOMBERG NEWS

Investigating the Allegations

- Credit Fraud Through Identity Theft
- Real Estate Fraud Through Identity Theft
- HIPAA Breach by Former Spouse
- Theft of Medical Services/Pharmaceuticals
- Social Engineering (telephone/online)
- Elder Abuse

Sources of Medical Identity Theft

- Family Member took ID
- Mail Theft
- Stolen or Lost Wallet/Purse
- Malicious Employee in Provider's Office
- Data Breach
- Phishing Attack

Resolving Medical Identity Theft

- Contact Health Plan/Insurer
- Contact Health Care Provider
- Contact Credit Bureaus
- Engage Identity Protection Service
- Contact Law Enforcement
- Contact Financial Institution(s)

How to Prevent Medical ID Theft

- Never Share Medical Identity Number
- Secure Personal Records at Home
- Shred Confidential Documents
- Locking Mail Box or P.O. Box
- Monitor Credit Reports
- Review Medical Records
- Do Not Respond to Phone/Online Surveys

Medical Identity Fraud & Theft

- Medical Identity theft occurs at a rate of .68% of the population
- Approximately 1.85 million Americans affected by this crime annually
- Using a mean total cost of $22,346 per incident derived from survey responses, estimated economic impact of medical identity theft in the United States at $41.3 billion per year.
- This represents a substantial increase from 2011 where the estimated total cost based on mean value of $30.9 billion dollars.

Source: *Ponemon Institute© Research Report, Third Annual Survey on Medical Identity Theft*

How Kaiser Permanente is Proactive

- Established a National Identity Theft Prevention Policy
- Check photo ID when patient appears for care – developed a “Check ID Toolkit”
- Effective Compliance Program and Hotline
- Excellent Forensic IT Tools
- Liaison with Law Enforcement
- Communicate What Happens to Perpetrators (terminated and prosecuted)
- Engage in Targeted Proactive Data Mining

External Reporting Requirements

- CMS Annual Part D Fraud, Waste, and Abuse Report
- CalPERS Kaiser Permanente National Fraud Control Annual Report
- Federal Employee Health Benefit Plan/Office of Personnel Management National Fraud Control Annual Report
- California Dept of Managed Health Care Anti-fraud Report, Kaiser Foundation Health Plan, Inc., California Regions
- California Department of Insurance
- Maryland and District of Columbia Departments of Insurance

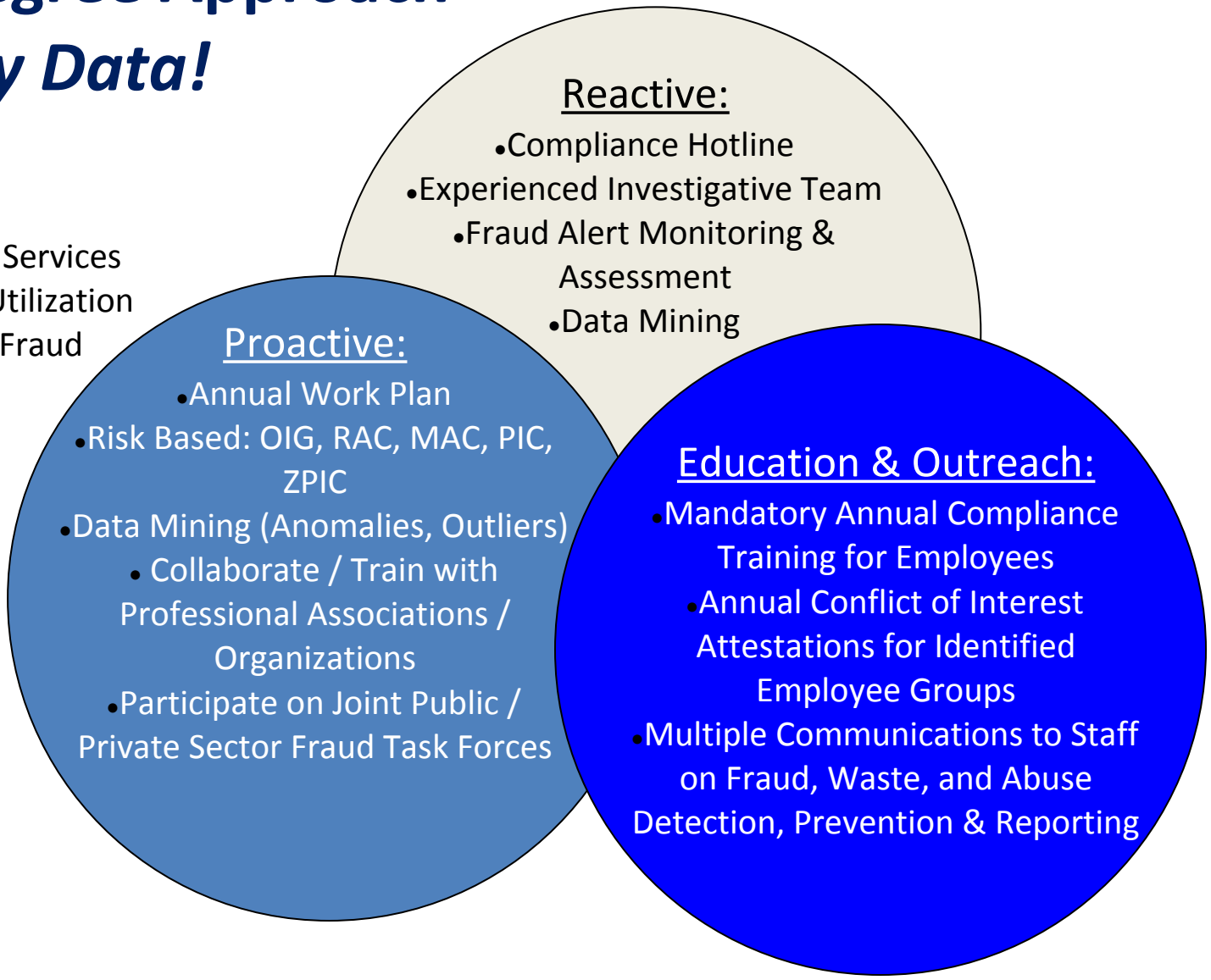
Changing Enforcement Environment

- In 2010, the Centers for Medicare and Medicaid Services (CMS) expanded its focus on enforcement through auditing and data mining to identify potential false claims
- An industry wide doubling of False Claim Act denials and recoveries has been forecasted
- CMS plans to expand audits in Medicare Advantage and Medicaid programs
- CMS has engaged Recovery Audit Contractors (RAC) to assist with identification of identity issues

A 360-Degree Approach
Driven By Data!

Hot Topics:

- Identity theft
- Theft of Medical Services
- Drug Seeking / Utilization
- Financial Theft / Fraud

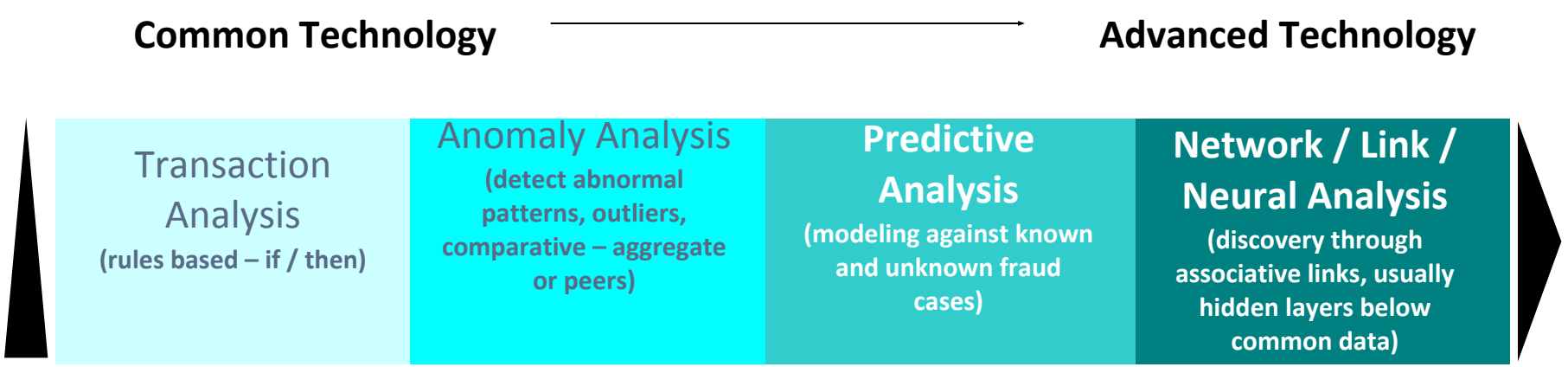


Data Approach: Our Data Footprint

- **Counts and amounts:**
  - Over 60 terabytes of non-encounter data
  - Eight categories with 69 active data sources
  - 5,605 tables
  - 143,243 columns
  - 18.8 billion records
- **Data is refreshed:**
  - Daily 4 sources
  - Bi-weekly 14 sources
  - Monthly 44 sources
  - Quarterly 6 sources
  - On-demand 3 sources

- **Pharmacy data:**
  - > 1.2 petabytes
  - All Rx's up to 15 years
  - Utilization & pricing data
- **Encounter data:**
  - > 900 terabytes
  - All encompassing: Physician notes, Laboratory, Radiology, Pharmacy orders, etc.

Data Mining Analytics Continuum



Drug Seeking Behavior and Drug Utilization

Summary and Definitions

SCAL - Weighted Drug Seeking Behavior (WDSB)		
Timeframe 5/1/2012 - 4/30/2013		
#	Pivot Table Name	Table Measures Description
1	**Top 10 Patients by Rank (Average Score > 30 OR Average MED / Day > 120)**	✓Patient Rank of 30 or greater is calculated by an overall weighted score comprised of: **(This is based on historic drug seeking behavior cases as investigated by pharmacy, iACT, and special investigations and industry)** 1. Distances between care of service (patient, pharmacy, physician) and medical office visits 2. Member Status: Active vs. Inactive 3. Prescribing Physician Count 4. Total Pharmacy Count 5. Calculated dose per day 6. Calculated prolonged usage **Plus 16 additional drug seeking behavior flags and behavior criteria** ✓ If the MED is 120 or greater and the score is low, we include this patient. Thus adding to CMS compliance ✓ Patient Average MED (Morphine Equivalent Dose) calculation as noted below in #2.
2	**Top 10 Patients by Total Morphine Equivalent (MED)**	ü Patient Total Morphine Equivalent is calculated by taking the sum of Script MED for all scripts for the same Patient and Drug Name where the Script MED is: **Quantity Dispensed * Total Mg * Morphine Factor** (see below for Morphine Factor table)
3	**Top 10 Patients by Average Morphine Equivalent (MED)**	Patient Average MED (Morphine Equivalent Dose) calculation as follows: **NOTE: if patient is on the drug for the entire 12 month period we use 365 as the divisor** If less than a 12 month period: Total MED / Days Supply where: Start Date = Fill Date End Date = Fill Date + Days Supply. [Calculate the Days Lapsed as Max(End Date)–Min(Start Date). For the divisor, use either the Days Lapsed or Total Days Supply, whichever is less]
4	**Top 10 Patients with Emergency Department Ordered Back Office Injections**	A count of Class-II Injections ordered as part of the Emergency Department admission for the same day as admission which could include multiple admissions. Detail of all ED injections are available in a separate document.
5	**Top 10 Patients with Urgent Care Ordered Back Office Injections**	A count of Class-II Injections ordered in Urgent Care which could include multiple visits. Detail of all UC injections are available in a separate document.
6	**Top 10 Patients by Longest Time Between "Visit Type" Encounters Only**	A search of all patient encounters where the encounter type was an actual "VISIT" and calculates the last visit date to end of study date to get number of days.
7	**Top 10 Patients by Greatest Tablet Count**	A count of all patients dispensed tablets (using the quantity field) returned meeting all criteria.
8	**Top 10 Patients by Greatest Liquid Volume**	A count of all patients dispensed liquid medication in mL (using the quantity field) returned meeting all criteria.
9	**Top 10 Providers Identified in Study**	A count of all prescriptions under a Primary Care Providers (PCP) Patient Panel

MED (Medical Equivalent Dose) of opioids: A standard representation of morphine drug equivalency calculated by converting a beneficiary's total opioid medications to their MED, i.e. a beneficiary's cumulative prescription opioid daily dose. (CMS has issued a threshold of 120 MED per)

Drug Utilization Review – Sample Reports

Reports to Clinicians for Drug Seeking Behavior (narcotics) to Meet Medicare & Other Requirements for Drug Utilization Review

Top 10 Patients by Rank (Average Score > 30 OR MED > 120)

MCA	MRN	Patient Name	Age	Rank	Avg Score
PAN	OM:-	3157mc-1G1N,A51525A5mc	71	1	64.61
BAK	bYo:}psOM	1015N57,mc-113 !	65	3	60.48
SUN	bOMYo:}Yo	105L-13H,!A51G1N Z	63	4	60.00
RIV	FFbOM:-	A5113-1A55Z,71LV1!15A5 13	41	5	59.29
RIV	bOM:-	A5H-1N5,!15NN1	71	6	59.23
SD	b:-}89OM:-	!5!5A5-11N,5L-1Z125mcH Z	72	7	59.19
SD	psYo:}8Yo:	13-1LL5A5,131A53-11 K	66	8	59.17
SD	bYo:}F8OM	65Lmc15N,L1A535LL-11	68	9	58.57
SD	FFFb0OM:-	131A5K7 10A5,:-)1Lmc5A5 :-)	66	10	58.18
BAK	psb9Fb90	!-11Z,L-1N!1	70	11	57.88

Top 10 Patients by Total Morphine Equivalent (MED)

MCA	MRN	Patient Name	Age	Total MED in mg	Avg MED in mg
BEL	bbYo:}9ps	!1LH15V5A5,31mcH5A5-1N5	54	825,000	2,500.00
ANA	bb8Yo:}0	!5L315Nmc,1NmcH15NY 13	50	773,430	744.40
SD	:-}8bOM:-	2A51515K7,!15L15A557	81	695,368	944.79
SD	bOM:-	:-)-175,1011357	74	654,000	905.82
ANA	:-	713-1mcH,G:-)5N5V5A55 L	63	574,200	1,698.82
RIV	b80:-	3161A515,K5LLY 13	49	526,500	731.25
SD	9F89Yo:}0	:-)A5-1GHmc,!-11N5 13	55	517,640	643.83
RIV	OM:-)ps:-):-	215N75-1GN5:}A5,A55G-1N1	57	508,060	471.30
ANA	bOM0bOM	61L315,7H1:}N1	58	493,350	527.65
BPK	}OMps0	57mcA51!1,13-13H15L 3	55	466,300	626.75

Top 10 Patients by Average Morphine Equivalent (MED)

MCA	MRN	Patient Name	Age	Avg MED in mg	Total MED in mg
BEL	bbYo:}9ps	!1LH15V5A5,31mcH5A5-	54	2,500	825,000
ANA	:-	713-1mcH,G:-)5N5V5A55	63	1,699	574,200
FON	OMOM:-	G1A5N5A5,A515N1L!	62	1,200	216,000
SD	:-}8bOM:-	2A51515K7,!15L15A557	81	945	695,368
WOD	Yo:}bYo:}Y	133L15:}GHL-1N,13-	57	939	384,900
FON	:-):-)b9OM:-	7315mcmc,7mc5V5N	57	933	166,000
SD	bOM:-	:-)-175,1011357	74	906	654,000
SD	OM:-	6152:}A5,131A5K A5	53	886	38,100
AV	bb9OM:-	H1K5N715N,1NN5 13	59	852	169,600
FON	}b0b9:-	:-)H55L5A5,3-1N!Y 13	52	847	224,400

Top 10 Patients with Emergency Department Ordered Back Office Injections (*Migraine DX)

MCA	MRN	Patient Name	Age	Rank	ED Inj
HAR	}psb	10	54	5439	123
WLA	sOM	H1A5A5-17,1015HN A5	30	7642	106
FON	}±bOM:-	Z-1675A5,KA5-17mc-1N1 13	29	5773	78
SD	}OM9	131A5mc-1N,13-13H15L 1	43	5362	76
WLA	}OMFOM:-	N51L,GL15A5-11 6	66	4123	74
ANA	b89b:-)F8	1LV57,K5-1mcH 1	49	5908	68*
AV	}F	G1!215-17,105NN-165A5 L	44	66	57*
WLA	}OOMOM:-	21522-1mcmc,	34	5493	55
SD	M:-)F0	73HA5155!5A5,1N!A55:-)6	30	23517	54
SUN	}Ob9OM:-	1N!1 7	61	4581	48

Top 10 Patients by Greatest Liquid Volume (Time Frame 5/1/12 - 4/30/13)

MCA	MRN	Patient Name	Age	Total Liquids	Liquid ML / day
HAR	}OYo:}0	L1L-125A5mc5,6A55!5A5-	66	81,000	221.92
SD	}9Yo:}F	25N715N,!1V-1! A5	65	19,866	54.43
SD	}8Yo:}b99	713-1mcH,61:}L G	81	17,974	49.24
RIV	}OM:-)OM	:-)A5-1GHmc,mcH5A5571	67	13,314	36.48
ANA	8OM:-)	6-1N5-1A515,mc1513171	91	12,911	35.37
WOD	}F:-)OM:-)	H125A5,L1:-)A55N35 H	72	10,800	29.59
ANA	}Yo:}b8ps:-	157215A5N5,7H-1A5L5Y 13	82	9,600	26.30
FON	}8OM:-)b±	7mc15HL5A5,25mcmcY 10	75	9,000	24.66
FON	}OF	6-17H5A5,5 H	83	7,500	20.55
RIV	}Yo:}OM8	L1 3157mc5,G:-)5N!15LYN	71	6,668	18.27

Top 10 Patients by Longest Time Between "Visit Type" Encounters Only (e.g. 4/30/2013 - Last Visit Date)

MCA	MRN	Patient Name	Age	Last Visit Date	# of Days
SD	}OM:-)	13K,131A5G1A55mc	86	1/4/2008	1943
SD	OMb8	21-1A5,!1A5A55LL 1	62	1/15/2008	1932
HAR	}OMb90	51325A5Y,25V5A5LY 10	84	5/13/2008	1813
SD	}ps8OM09	761:}L!-1NG,315A5-1	82	6/6/2008	1789
N/A	}F9bbb	!A55:-),LYNN5	72	5/11/2009	1450
WOD	}080OM:-)	3H-1N,mcH151317 1	60	9/23/2009	1315
HAR	}OM:-):-)9F	A555V57,L-122Y	89	10/20/2009	1288
RIV	}±9OM:-)b	mc-13KN5A5,1013K 5	75	11/17/2009	1260
SUN	}OM:-)OM:-	G1A5N-1GH-113	93	3/3/2010	1154
RIV	FFYo:)	N715N,13-13H15L H	61	4/21/2010	1105

Drug Utilization Review – Sample Reports

Reports to Clinicians for Drug Seeking Behavior (narcotics) to Meet Medicare & Other Requirements for Drug Utilization Review

Top 10 Patients by Greatest Tablet Count (Time Frame 5/1/12 - 4/30/13)

MCA	MRN	Patient Name	Age	Total Tablets	Tablets per day
BPK	b0FYo:}:-	57mcA51!1,13-13H15L 3	55	24380	67
SD	9F89Yo:}0	:-}A5-1GHmc,!-11N5 13	55	24285	67
ANA	bbOMOM	31A5131N,2A5-11N 3	67	18600	51
RIV	OM:-}ps:-}:-	215N75-1GN5:}A5,A55G-1N1	57	16170	44
FON	88:-	L:}K57H,:-}1Lmc5A5 10	48	14600	40
WOD	Yo:}bYo:}Y	133L15:}GHL-1N,13-13H15L	57	12830	35
SD	bYo:}FYo:)	L:}35A515,L:}3Y L	44	12788	35
SD	8bFYo:}9p	65A5G:}715N,!1V-1! :-)	52	11520	32
SD	9:-}:-	713-1mcH,131A5Y !	69	11160	31
ANA	M:-}:-}80	!5L315Nmc,1NmcH15NY 13	50	10875	30

Top 10 Patients with Urgent Care Ordered Back Office Injections (*Migraine DX)

MCA	MRN	Patient Name	Age	Rank	UC Inj
RIV	bOMFYo:}b	7-1525A5,N-1N1 L	53	7542	28*
WLA	OM:-}Yo:}:-	G-1227,1011357 13	44	3655	12*
AV	bFb:-	131LL15A5Y 6A551mc15A5,K-	47	7908	10
AV	b0F0bOM:-	G1!215-17,105NN-165A5 L	44	66	9*
AV	9b9Yo:}0	75A5G5Y,mcH151317	53	8449	9
ANA	b89b:-}F8	1LV57,K5-1mcH 1	49	5908	8*
AV	OM:-}:-	73H1NL5Y,!-11NN5	69	6325	7*
BAK	bYo:}Yo:}b	:-}-1L715N,5L-1Z125mcH 10	49	19137	7
N/A	Yo:}OMps	133K-1NN15N,G5A51L! 10	79	3532	6*
ANA	}ps0FF:-)	2A515:-}N,10:}!-1mcH 5	68	5794	6

Top 10 Providers Identified in Study

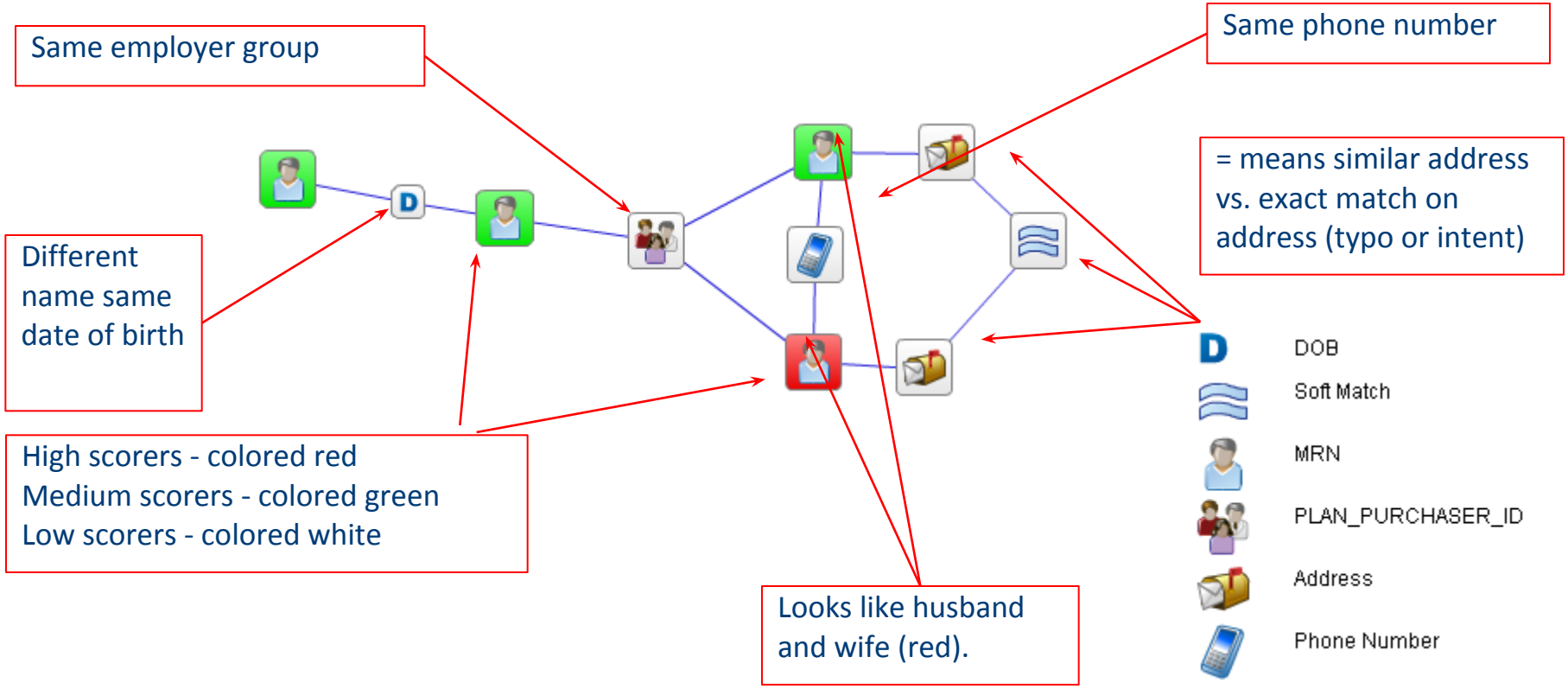
MCA	PCP	PCP Email	RX Count
FON	L-1:}, L57 -1 L55 (13.!.)	L57.-1.L-1:}@K6.15A5G	468
SD	G15L!5N, 1N!A55:-) 13Y5A57 (13.!.)	1N!A55:-	457
RIV	13-15LK5, K5V-1N 1015N (!.15.)	K5V-1N.10.13-	442
FON	mc15153H-1N!1, 3H1A55A5Nmc17	mc17.X.mc15153H-	428
BAK	:-}15NG, 3H1A5Lmc15N (13.!.)	3H1A5Lmc15N.:-	396
BAK	mc55mc5N, 7mc1NL5Y (13.!.)	7mc1NL5Y.X.mc55mc5N	378
BAK	5N153H, A5:}775LL 51A5L (!.15.)	A5:}775LL.5.5N153H@K6.	368
N/A	NONE	NONE	359
BAK	3H:}1NG, 65L-1X 3 mc (13.!.)	65L-	351
FON	71V5A5Y, 7H5A5-1LYN 101377:}5L-	7H5A5-	334

MED (Medical Equivalent Dose) of opioids: A standard representation of morphine drug equivalency calculated by converting a beneficiary's total opioid medications to their MED, i.e. a beneficiary's cumulative prescription opioid daily dose. (CMS has issued a threshold of 120 MED per)

Data Analytics: Link / Network Analysis

How to interpret a network diagram:

The goal of Link Analysis (also known as social or network analysis) is to uncover potential member fraud networks by linking flagged members based on name, address, home phone number, employer (plan purchaser), and date of birth.



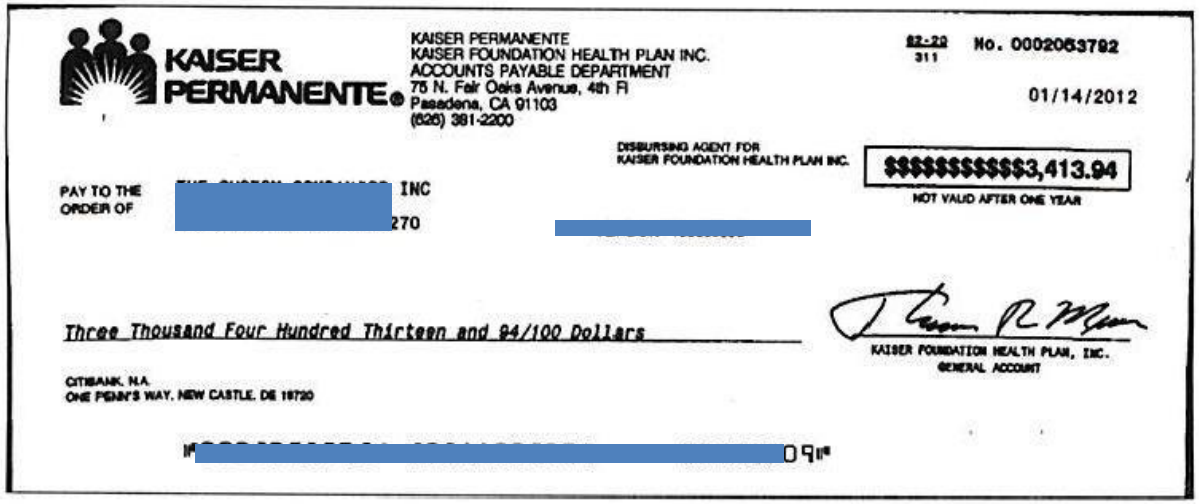
Fraud Control: Identity / Payment Fraud

citi

Print Close Window

Check Image Inquiry Results

Account #	Check #	Amount	Paid Date	Sequence #
[redacted]9	2053792	$3,413.94	01/24/2012	1100501404



KAISER PERMANENTE

KAISER PERMANENTE
KAISER FOUNDATION HEALTH PLAN INC.
ACCOUNTS PAYABLE DEPARTMENT
75 N. Fair Oaks Avenue, 4th Fl
Pasadena, CA 91103
(626) 381-2200

82-29
311

No. 0002053792

01/14/2012

DISBURSING AGENT FOR
KAISER FOUNDATION HEALTH PLAN INC.

$$$$$$$$$$$3,413.94

NOT VALID AFTER ONE YEAR

PAY TO THE ORDER OF [redacted] INC

270

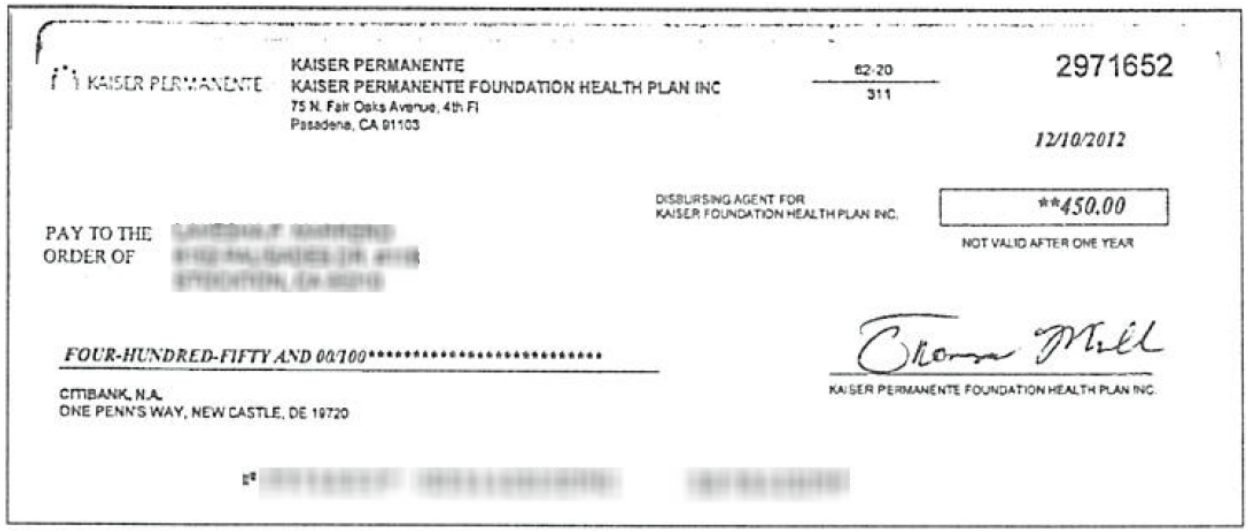
Three Thousand Four Hundred Thirteen and 94/100 Dollars

KAISER FOUNDATION HEALTH PLAN, INC.
GENERAL ACCOUNT

CITIBANK, N.A.
ONE PENN'S WAY, NEW CASTLE, DE 19720

[redacted]

Data Analytics: Link / Network Analysis



KAISER PERMANENTE

KAISER PERMANENTE
KAISER PERMANENTE FOUNDATION HEALTH PLAN INC
75 N. Fair Oaks Avenue, 4th Fl
Pasadena, CA 91103

62-20
311

2971652

12/10/2012

DISBURSING AGENT FOR
KAISER FOUNDATION HEALTH PLAN INC.

**450.00

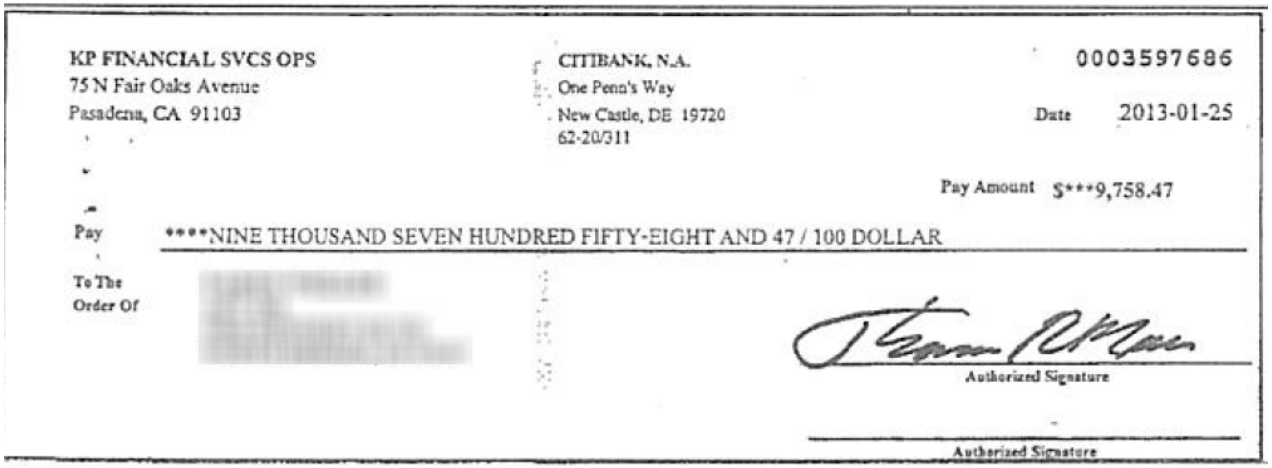
NOT VALID AFTER ONE YEAR

PAY TO THE
ORDER OF

FOUR-HUNDRED-FIFTY AND 00/100**********

CITIBANK, N.A.
ONE PENN'S WAY, NEW CASTLE, DE 19720

KAISER PERMANENTE FOUNDATION HEALTH PLAN INC.



KP FINANCIAL SVCS OPS
75 N Fair Oaks Avenue
Pasadena, CA 91103

CITIBANK, N.A.
One Penn's Way
New Castle, DE 19720
62-20/311

0003597686

Date 2013-01-25

Pay Amount $***9,758.47

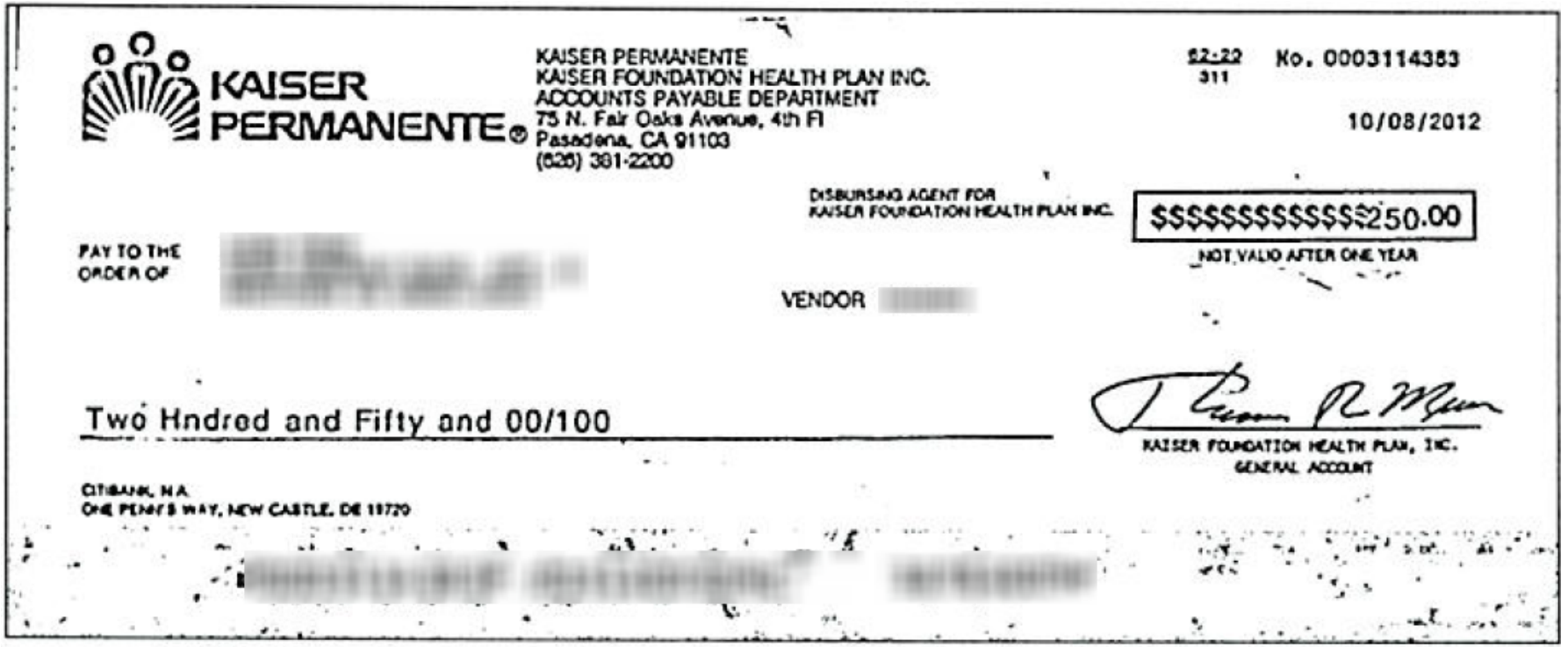
Pay ****NINE THOUSAND SEVEN HUNDRED FIFTY-EIGHT AND 47 / 100 DOLLAR

To The
Order Of

Authorized Signature

Authorized Signature

Data Analytics: Link / Network Analysis
Check Fraud



KAISER PERMANENTE

KAISER PERMANENTE
KAISER FOUNDATION HEALTH PLAN INC.
ACCOUNTS PAYABLE DEPARTMENT
75 N. Fair Oaks Avenue, 4th Fl
Pasadena, CA 91103
(626) 381-2200

52-22
311

No. 0003114383

10/08/2012

DISBURSING AGENT FOR
KAISER FOUNDATION HEALTH PLAN INC.

$$$$$$$$$$$$250.00

NOT VALID AFTER ONE YEAR

PAY TO THE
ORDER OF

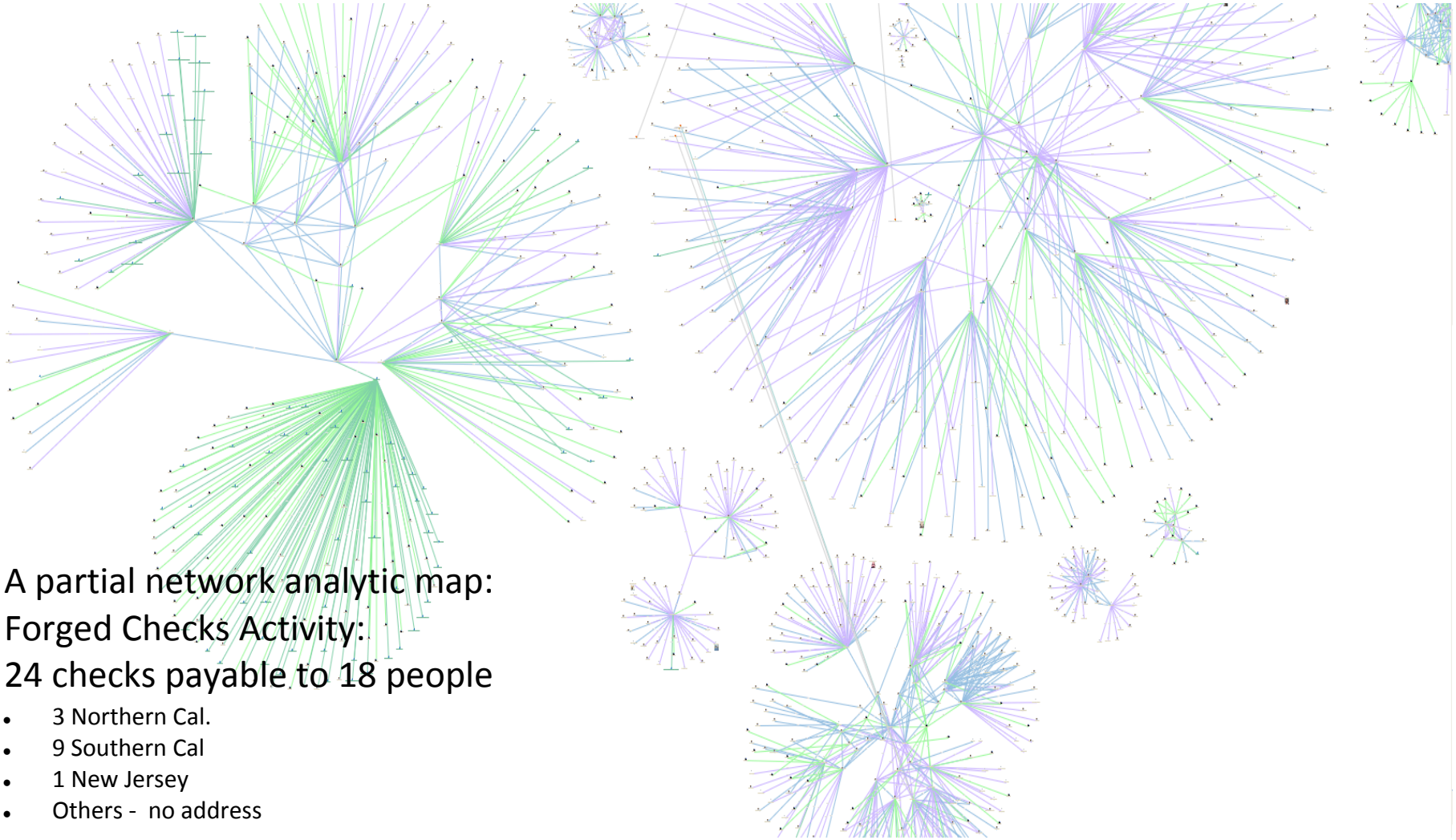
VENDOR

Two Hndred and Fifty and 00/100

KAISER FOUNDATION HEALTH PLAN, INC.
GENERAL ACCOUNT

CITIBANK, N.A.
ONE PENN'S WAY, NEW CASTLE, DE 19720

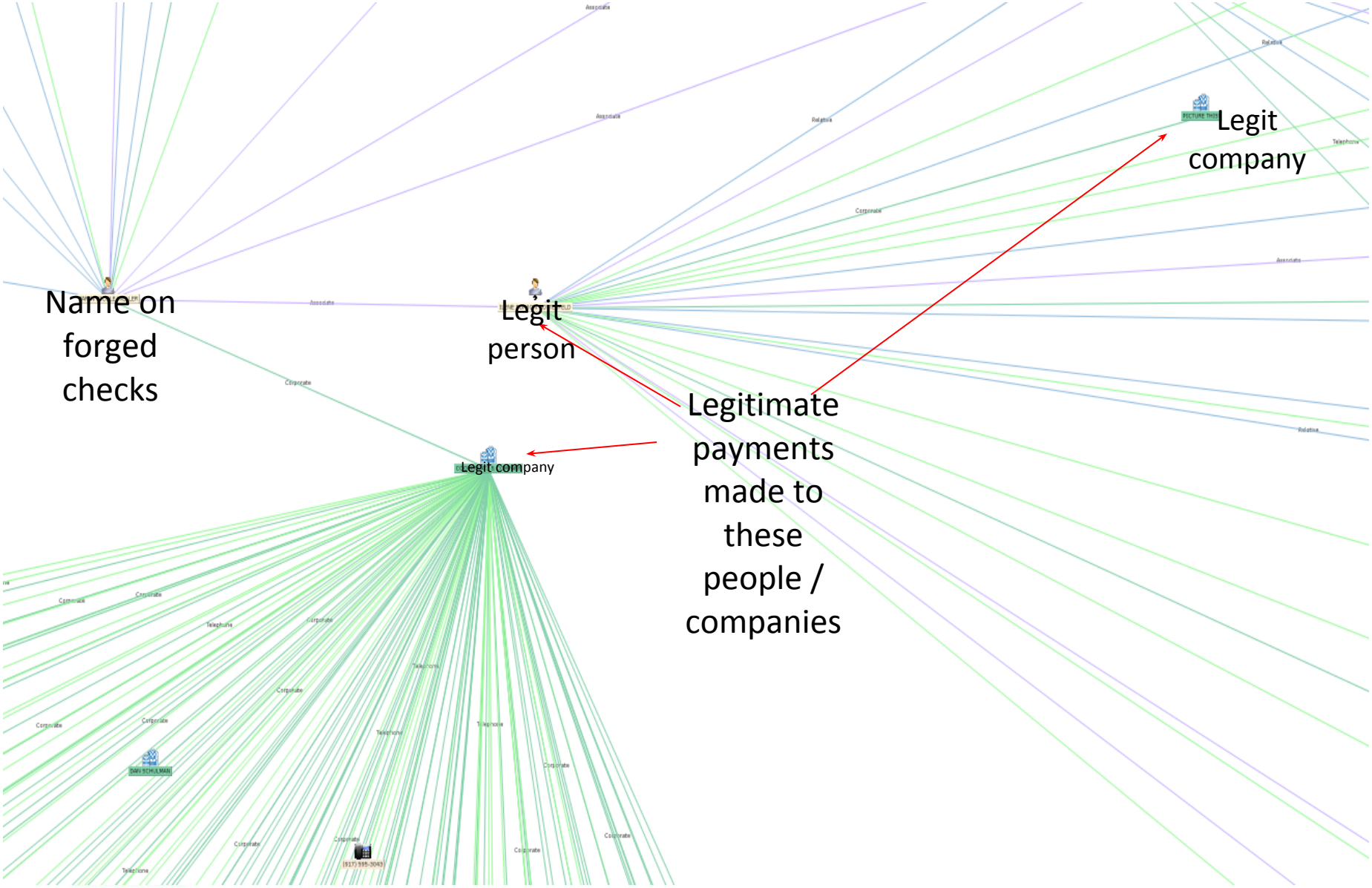
Data Analytics: Link / Network Analysis



A partial network analytic map:
Forged Checks Activity:
24 checks payable to 18 people

- 3 Northern Cal.
- 9 Southern Cal
- 1 New Jersey
- Others - no address

Data Analytics: Link / Network Analysis

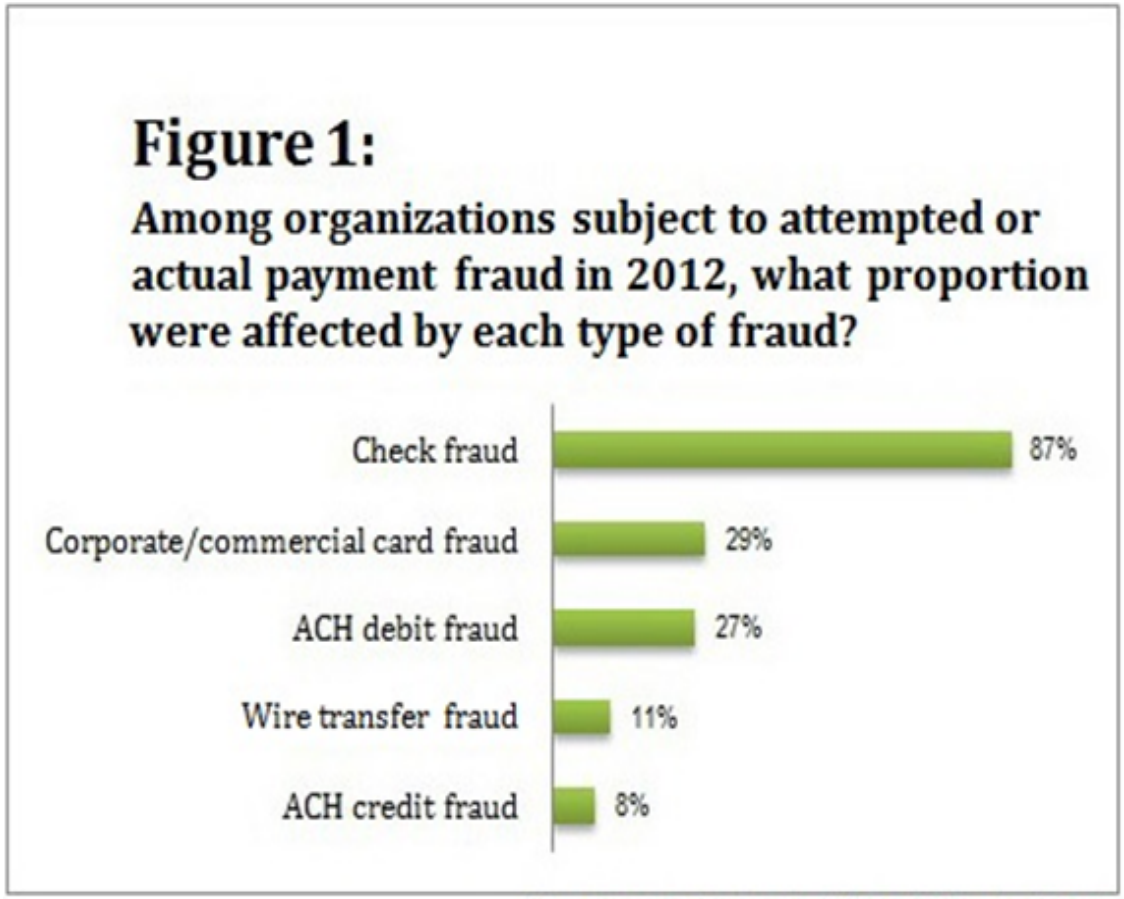


Fraud Control: Identity / Payment Fraud

2013 Association of Financial Professionals Survey:

- Payments fraud experienced by businesses remains persistent
  - 61 percent of organizations experienced attacks on payment systems
  - Checks continued to be the dominant payment form targeted by fraudsters
  - 87 percent of affected organizations reporting check fraud attempts
- Check fraud has been around for a long time, but in recent years criminals have become more proficient at it
  - The advent of inexpensive desktop publishing equipment has enabled them to create incredibly authentic-looking counterfeit checks
  - In its most common form, counterfeiting involves creation of fraudulent checks using an organization's MICR-line data
  - Criminals also commonly alter the amount or payee name on checks that have actually been issued, or they steal or counterfeit employee paychecks

Fraud Control: Identity / Payment Fraud



Source: Association for Financial Professionals. "2013 AFP Payments Fraud and Control Survey."

A company has 24 hours to contact its bank to dispute a fraudulent ACH debit. Failure to initiate a dispute within the 24-hour window shifts all liability for fraud losses to the corporate account holder.

Data Mining for Comprehensive Application Access Monitoring

System access type algorithms in use:

- User accesses adult medical records from a pediatric position
- User accesses male records from an OB-GYN position (not part of fertility treatment)
- User accesses medical records shortly after patient checks out for no medical reason
- User accesses records of patients with same name as they have
- User accesses records of patients never cared for at their clinic or hospital
- User accesses demographics of records when that is not part of their job (e.g. phlebotomist does not need to know where

Monitoring HIPAA compliance / identity theft

- User prints a very high number of medical records for position assignment
- User views medical record numbers sequentially and this is not part of the position or assignment
- User changes elements in a medical record that do not change (e.g., blood type, date of birth)
- User accesses records when there is no corresponding medical visit
- User accesses records of patients who are no longer health plan members

Fraud Control: Online Banking

Online Banking: New Opportunities for Fraud

- In recent years, a new type of ACH fraud has emerged as criminals have taken advantage of companies' adoption of online banking.
- New online banking scams are introduced almost daily.
- "Phishing." - someone receives an email from what appears to be a trusted business partner, such as a bank.
    - The email may ask the reader to open an attachment or click a link. The website the reader lands on may appear to be legitimate, but in actuality it's a counterfeit site. Once on a counterfeit site, a treasury professional may be asked to divulge bank account numbers and online banking credentials, such as usernames and passwords.
- "Reverse phishing," begins when a corporate staff member receives an email that appears to be from a known vendor. Rather than asking for online banking credentials, the message's sender asks the recipient to take an action, such as redirecting an electronic trade payment to a different bank account.
    - The victimized company may not even realize it has been scammed until weeks later, when the actual vendor calls to ask why its invoice is unpaid.

Fraud Control: Online Banking

Security Tips for Online Banking for Treasury & Finance Staff

- Never open e-mails from unknown sources.
- Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious e-mail.
- Educate yourself about current scams and loss-prevention steps.
- Make sure all computers you use for work-related business—both in the office and at home—have the latest versions and patches of both anti-virus and anti-spyware software.
- Install all updates and patches that include security fixes for software such as Internet Explorer and Adobe Reader.
- Use strong, complex passwords.
- Change your passwords regularly, and use a different password for each website you access.
- Never reveal to anyone your confidential username, password, PIN, or answers to security questions.
- Never share your security token, and immediately report lost or stolen tokens.
- Never bank online using computers at kiosks, cafes, or anywhere in which the computer or wireless network is unsecured.

Source: Linda Coven, Capital One

Fraud Control: 2012 Top 25 Passwords - Online Banking

(Compared to 2011)

1. password (Unchanged)
2. 123456 (Unchanged)
3. 12345678 (Unchanged)
4. abc123 (Up 1)
5. qwerty (Down 1)
6. monkey (Unchanged)
7. letmein (Up 1)
8. dragon (Up 2)
9. 111111 (Up 3)
10. baseball (Up 1)
11. iloveyou (Up 2)
12. trustno1 (Down 3)
13. 1234567 (Down 6)
14. sunshine (Up 1)
15. master (Down 1)
16. 123123 (Up 4)
17. welcome (New)
18. shadow (Up 1)
19. ashley (Down 3)
20. football (Up 5)
21. jesus (New)
22. michael (Up 2)
23. ninja (New)
24. mustang (New)
25. password1 (New)

Source: CNN – 25 worst passwords for 2012

Fraud Control: Check Your Password

https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx

http://www.passwordmeter.com/

"There are new attacks every day, we see something like 90,000 new pieces of malicious codes coming into our labs every day -- that's one every second."

- Graham Cluely, Senior Technology Consultant, Sophos.

The best advice is to never use an ordinary word as a password. Cluely has a very simple method to ensure that passwords are more secure, easy to remember but difficult for hackers to crack.

Example of a strong secure password is "F&WL2HH&E4D."

"Fred And Wilma Like To Have Ham And Eggs For Dinner" becomes "F&WL2HH&E4D."

What to do	Example
Start with a sentence or two.	Complex passwords are safer.
Remove the spaces between the words in the sentence.	Complexpasswordsaresafer.
Turn words into shorthand or intentionally misspell a word.	ComplekspasswordsRsafer.
Add length with numbers. Put numbers that are meaningful to you after the sentence.	ComplekspasswordsRsafer201

Fraud Control: Check Your Password

My old password:

Wigolmhwi64w&mbyl&m

Contact Information

Tamara Neiman

National Compliance Ethics & Integrity Office
Director of National Special Investigations Unit
408.366.4554
Tamara.l.neiman@kp.org

Jay Loden

National Compliance Ethics & Integrity Office
Asst. Director, Information Analytics and Compliance Technology Department / Data Analytics
626.674.4476
jay.m.loden@kp.org