

'id:analytics™

Understanding What Really Happens to Identities After a Data Breach

Thomas Oscherwitz

Vice President of Government Affairs

ID Analytics, Inc.

June 3, 2008



Purpose of Data Breach Harm Analysis Study

- To build upon the research of the National Data Breach Analysis study (2005).
- To better understand the harm resulting from data breaches.
- To observe how fraudsters are currently using breached data.
- To identify technologies that minimize the harm from data breaches.



Executive Summary

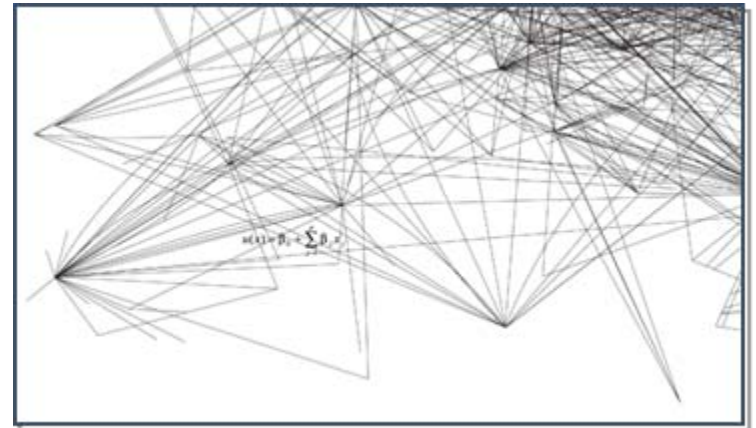
- Contrary to popular belief, most data breaches do **NOT** result in identity theft or misuse
- **Faceless transactions** are a breeding ground for fraud
- We found **no evidence of an active black market** for breached data
- Size of data breach did not significantly impact number of identities misused



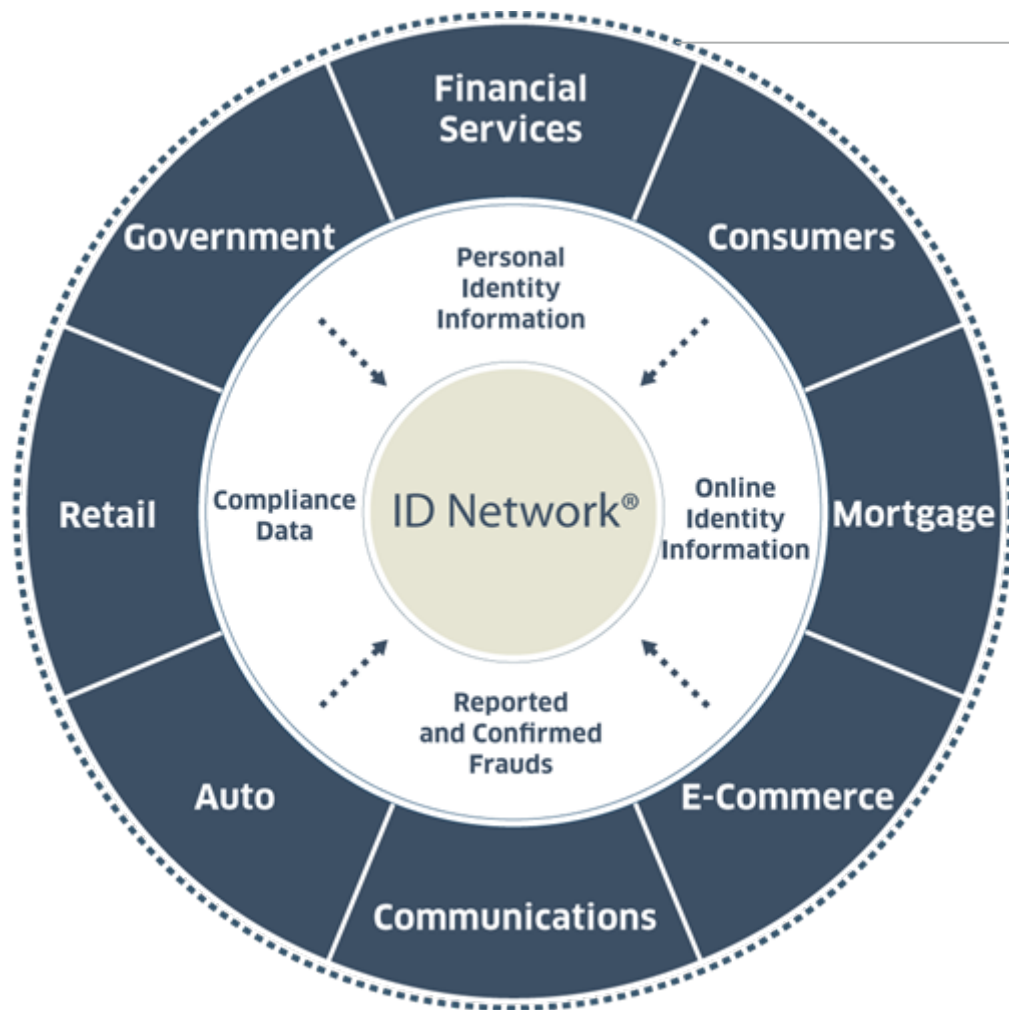
About ID Analytics, Inc.

ID Analytics Overview

- Leader in on-demand identity intelligence
 - Identity Risk Management
 - Compliance and Authentication
 - Customer Management
 - Credit Analytics
- Founded 2002
 - HQ San Diego, CA
- World class customer base
- Key strategic partnerships



ID Network®



ID Network

- First national, cross-industry compilation of identity information
- 360 billion total aggregated attributes
- 750 million unique identity elements
 - Average daily flow = 45 million
 - 2 million reported frauds
 - 1 billion consumer transactions
 - Contains information about:

Credit applications

Card transactions

Payments

Change of name/address

Demographics







Data is never sold or distributed

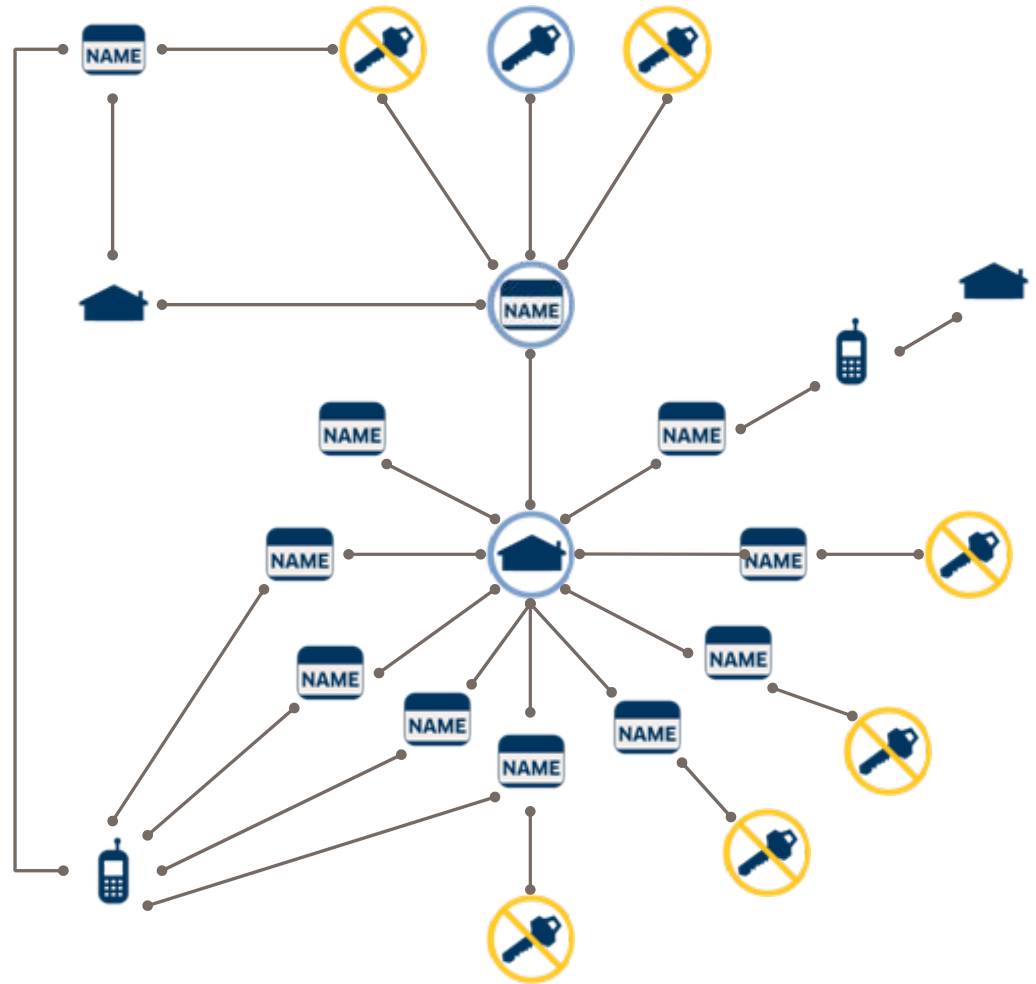
Real World Example

Date of birth occurs after
SSN issuance

10 people at this address,
invalid SSNs

2 apps on same day,
different addresses

-  Applicant Name
-  SSN
-  Address
-  Phone
-  Asserted Info on App
-  Invalid SSN



Identity Fraud – Criminal Attraction

Financial fraud

- \$6000 avg. new account fraud loss. Doubled from 2005-2006¹
- Auto loans, mortgage, tax returns and utilities
- Wireless: subscription fraud, equipment loss; account take over

Insurance fraud

- Auto, workers comp, life, health and disability

Healthcare benefits

- Estimated 250k Americans had health records stolen and misused²

Immigration fraud

- Employment related fraud accounts for 14% of stolen ID usage³

Identity manipulation

- Altering identity to hide negative events

Avoiding legal sanctions

- Warrants, child support and alimony

Identity fraud costs the U.S. about \$48-53 billion/year³

¹ Gartner, Survey, 2006; ² World Privacy Forum, Businessweek; ³ Federal Trade Commission, Report, 2006



National Data Breach Analysis

2005

National Data Breach Analysis: 2005

#	Breach Type	What Was Stolen?
1	Identity-Level, Targeted	Name, SSN, DOB, Phone #, Address
2	Identity-Level, Incidental	Name, SSN, DOB, Phone #, Address
3	Account-Level, Targeted	Name, Acct #
4	Account-Level, Targeted	Name, Acct. #

Are All Breaches the Same?

WHAT?

Account Level



James D. Hark
5402-1234-5678-9012
Expiration Date

Identity Level



James D. Hark
SSN 450-73-XXX
2372 Carroll Lane
Carmel, CA 92027
760-746-55XX
DOB 10/09/63

Are All Breaches the Same?

HOW?

Account Level

Identity Level

**Targeted
Access**



Intent to steal information

**Incidental
Theft**



Intent to steal goods

Lost Data

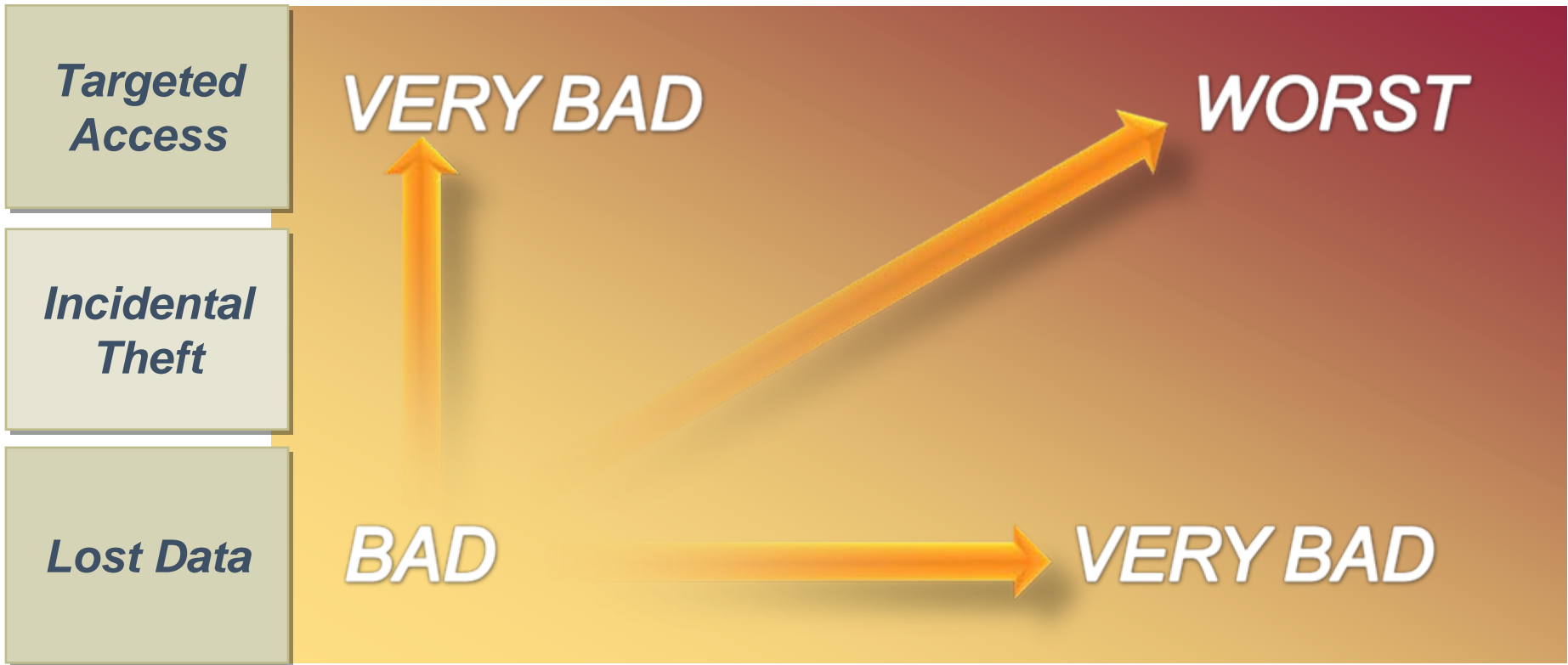


No real
intent

Is There a “Bad Scale”?

• Account Level

• Identity Level



Key Finding

The highest “misuse rate” was calculated at 0.098%

Less Than 1 In 1,000
Breached Identities
Were Misused

Key Finding: Sophisticated Fraudsters Use Stolen Identities at the Same Rate as Normal, Non-Breached Identities

Avg. Apps
Per Consumer:
1.3 Apps Per ID

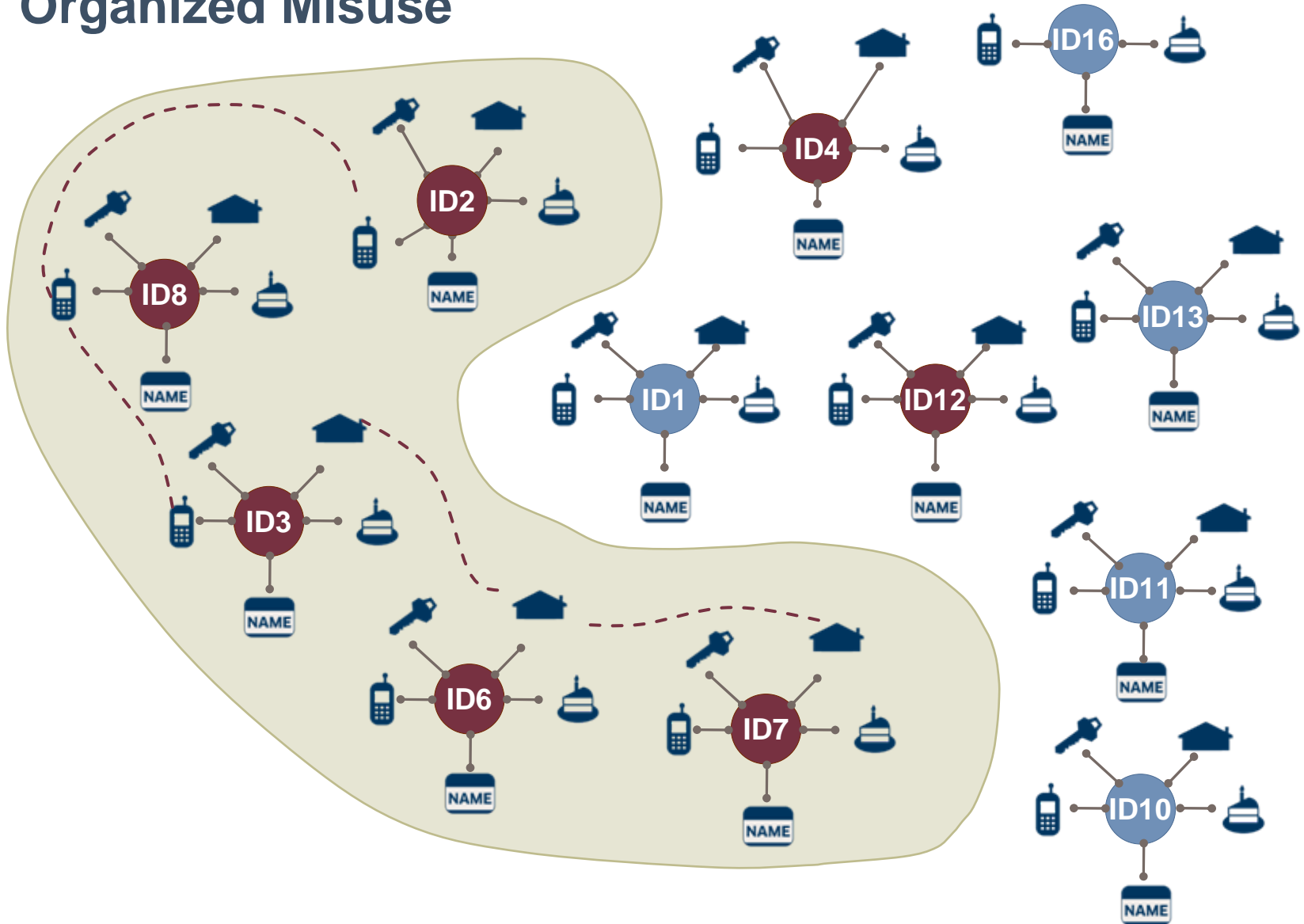
Avg. Apps Per
Breached ID:
1.3 Apps
Per ID





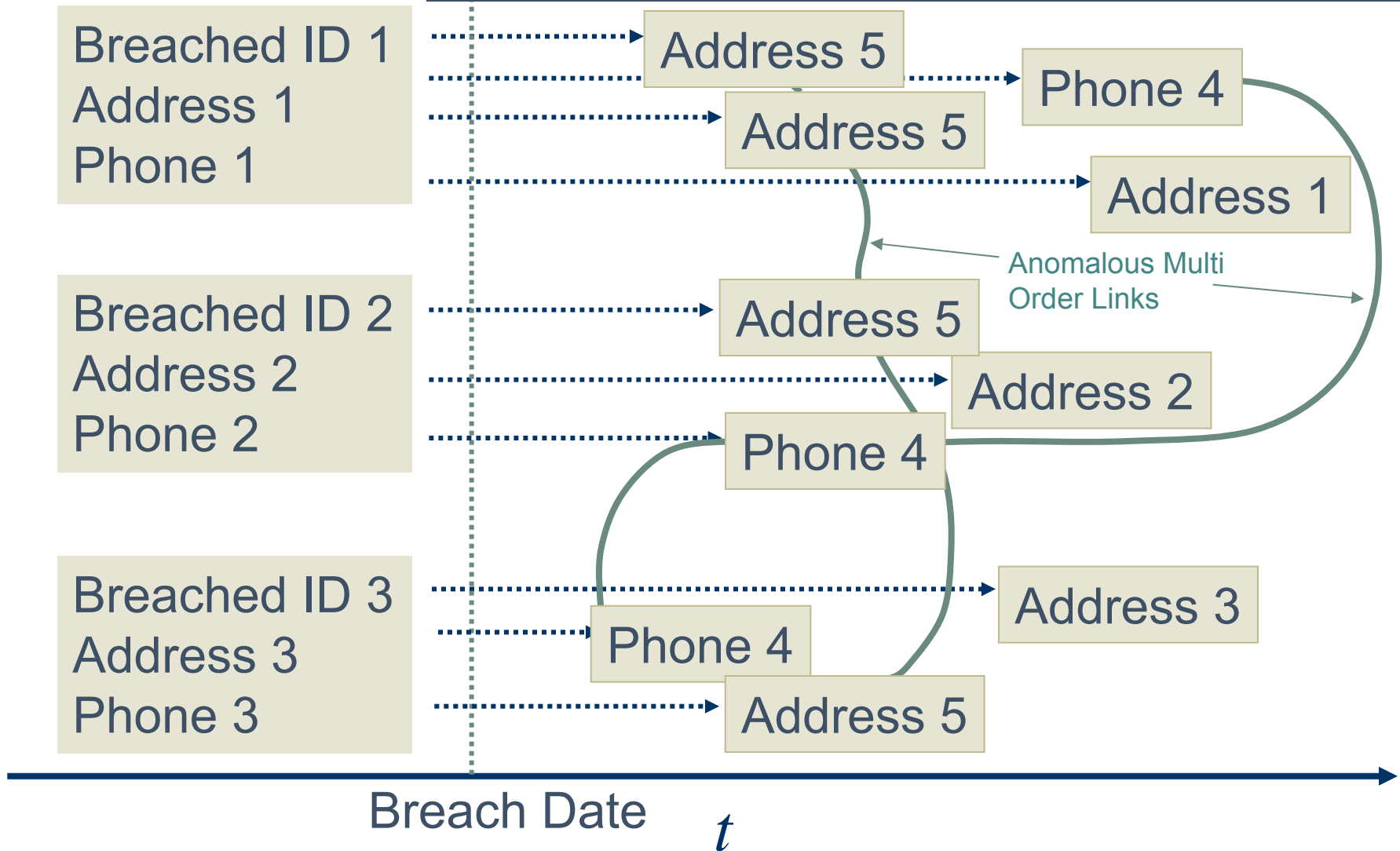
Methodology

Organized Misuse



Using the ID Network to Detect Misuse

“Events” received by ID Network post-breach





National Data Breach Harm Analysis

2007



What ID Analytics Studied

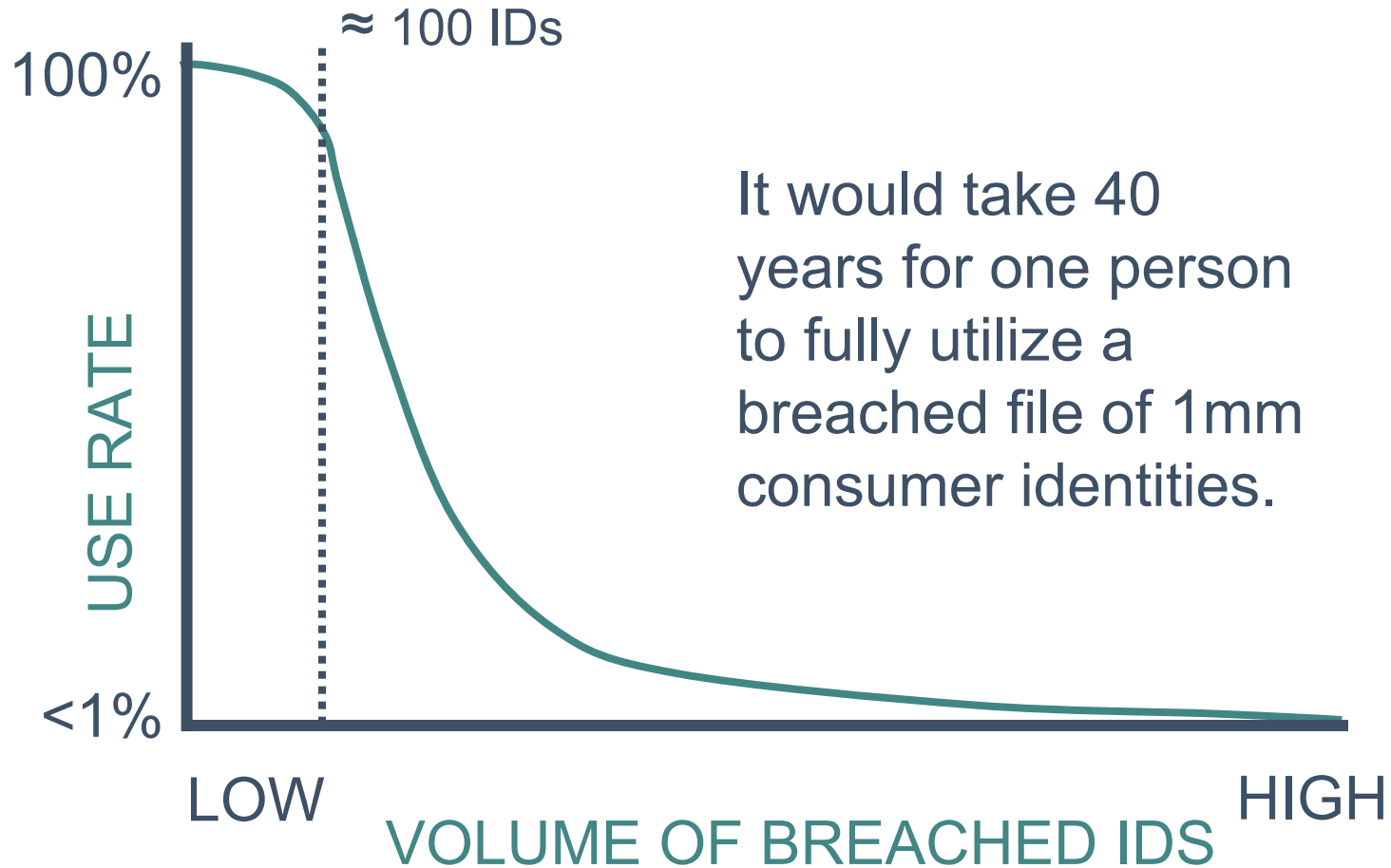
- Identity-level breaches only
- Over a dozen breaches involving more than 10 million identities
- Breaches varied widely in size
- Studied from six months to two years after incident
- Riskier than normal profile: typically involved stolen hardware or data



Harm Rate from Breaches

- Identified five cases of harm out of over a dozen breaches.
- Harm rates for five cases of misuse ranged from 0.01% to 0.5% of breach file.
- Highest harm rates found in smaller files.
 - File with highest misuse rate (0.5%) had less than 5,000 identities.
 - For every file greater than 100,000 identities, harm rate was less than 0.01%.

Key Finding: The Smaller the Breach, the More Likely the Consumer will be Affected





Common Patterns of Misuse

1. The lifespan of misuse involving a single compromised identity is typically less than two weeks.
2. There was no evidence that the data from any of the breaches was sold or widely distributed to others with criminal intent.
3. The patterns of misuse tended to link the breached personal data to a limited set of new phone numbers and addresses.
4. Misuse of the breached data tended to focus on fraudulent applications for credit cards through the Internet.
5. There is a link between employee theft and the geographic location of the misused identities.
6. More organized misuse occurred with new application for bank credit cards than applications for new wireless phones or retail credit cards.

Another Look at Lifecycle of Identities

Case of Misuse	Percent of Misused Identities with a Lifecycle LESS than 2 Weeks
1	90%
2	98%
3	71%
4	86%
5	100%



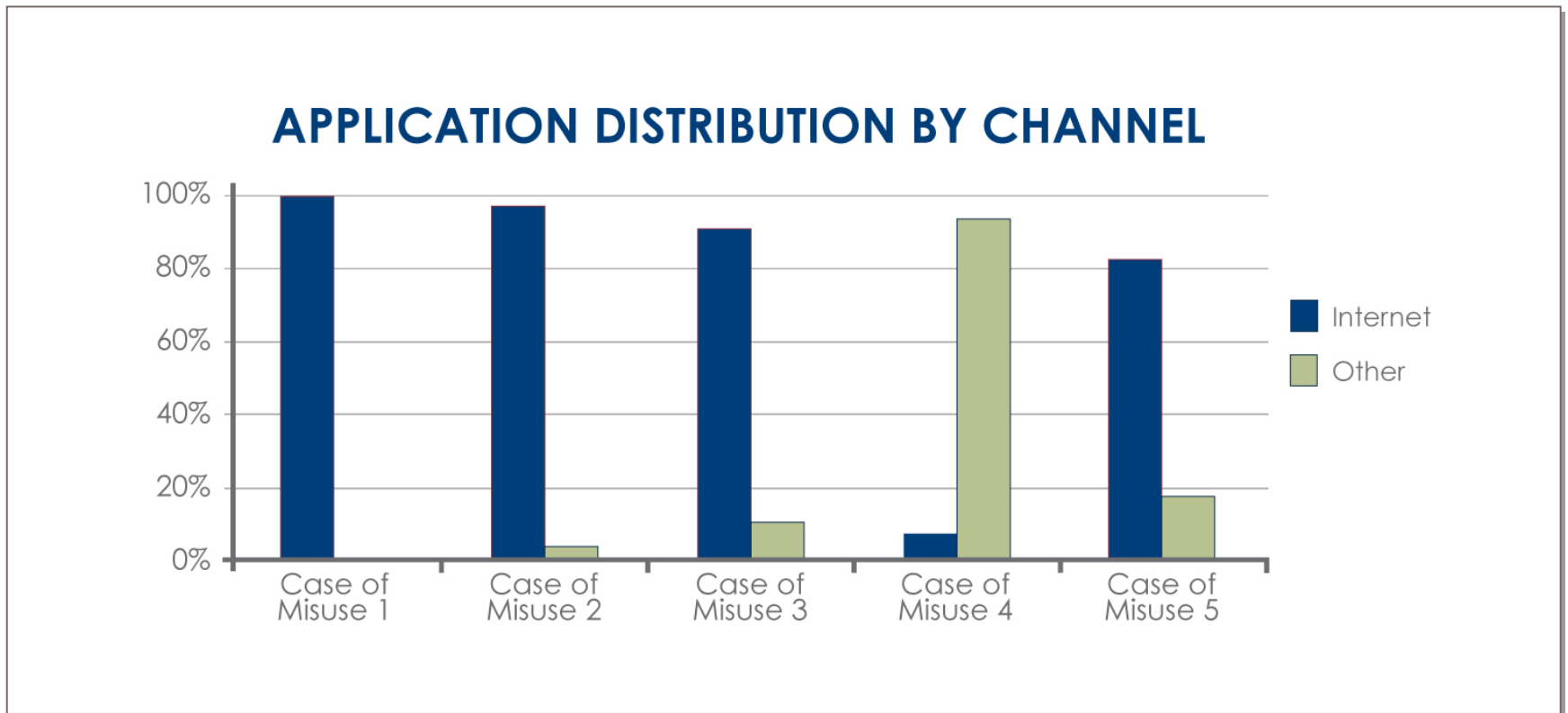
2. Breached Data Not Widely Distributed

- Is breach data being sold widely on the black market?
- Hypothesis: With an active black market for data, we would have expected to see unrelated pockets of misuse in the files
- What we found: No evidence of widespread misuse of data. Misuse activity suggested the work of a single fraudster for fraud ring. Fraud centered around a limited number of related phone numbers and addresses.
- Snapshot: We are seeing current fraudulent behavior. Cannot predict the future.

3. Organized Misuse Clustered Around Few Points of Contact

Case of Misuse	Addresses	Phones	Identities	Applications
1	5	1	69	198
2	1	6	98	149
3	2	8	41	110
4	13	2	22	28
5	10	1	24	39

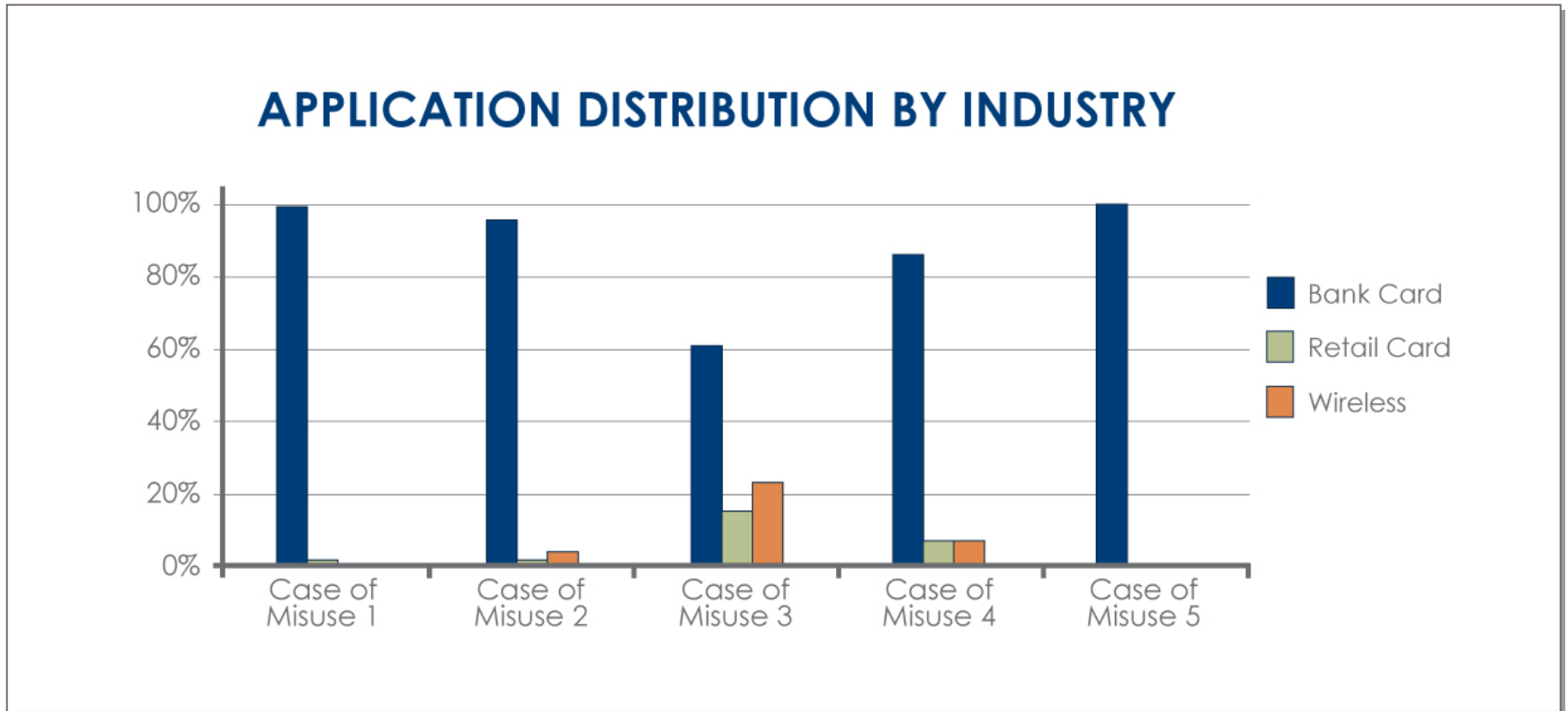
4. Fraudsters Use the Internet to Obtain Credit Cards



5. Internal Data Theft is Linked to Geographic Misuse of Data

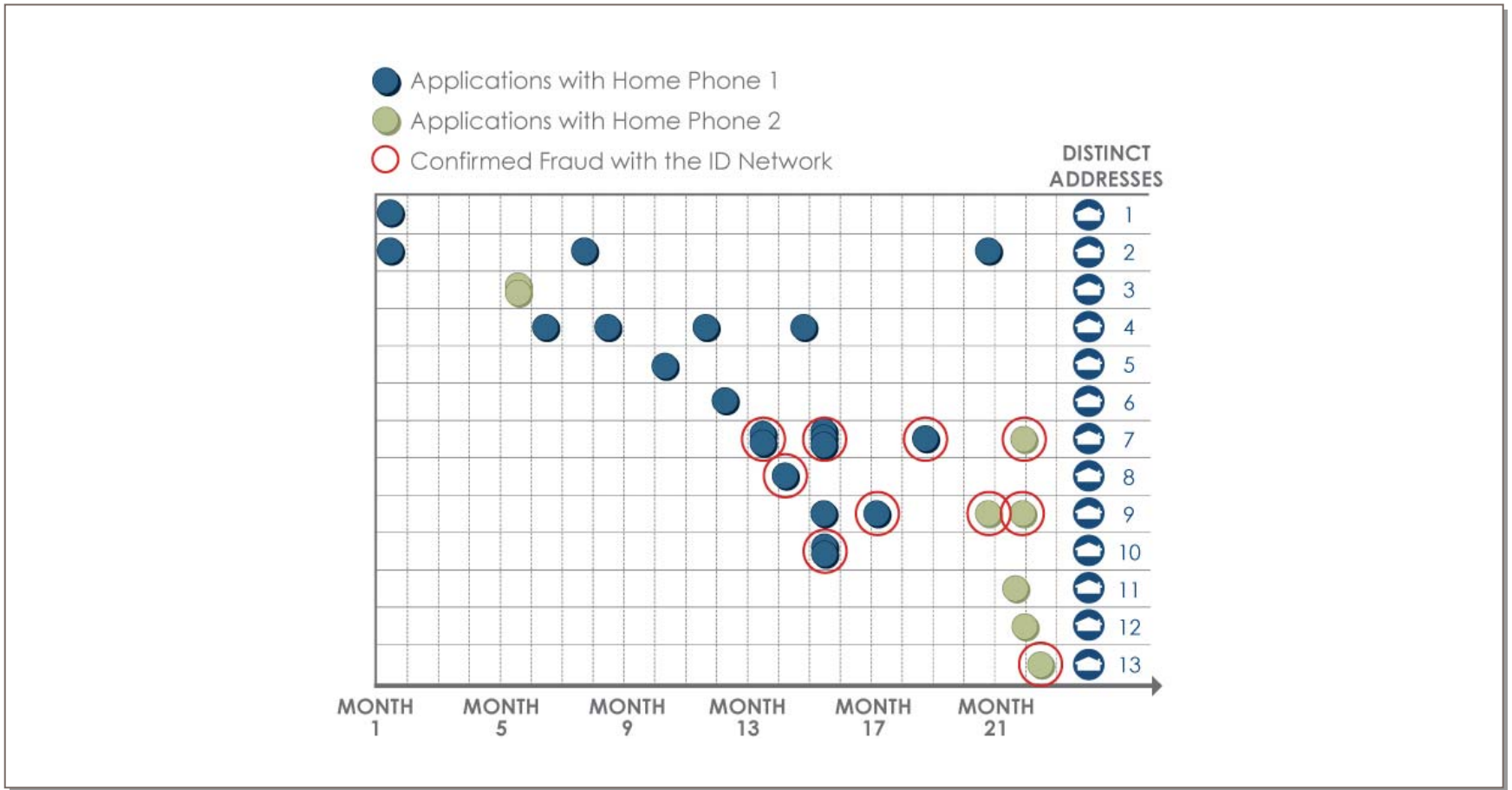
- In 2 of 5 cases of misuse, an employee stole data.
- Both cases, resulting misuse occurred with identities and addresses close to the worksite.
- In one case, perpetrator targeted identities with addresses between 2 and 5 miles from worksite.
- Fraud from internal sources still one of the great unknowns.

6. Fraudsters Favor New Applications for Credit Cards Over Retail Credit Cards or Wireless Phones



Case Study

Application Velocity Across Home Phones and Addresses





Common Patterns of Misuse

1. The lifespan of misuse involving a single compromised identity is typically less than two weeks.
2. There was no evidence that the data from any of the breaches was sold or widely distributed to others with criminal intent.
3. The patterns of misuse tended to link the breached personal data to a limited set of new phone numbers and addresses.
4. Misuse of the breached data tended to focus on fraudulent applications for credit cards through the Internet.
5. There is a link between employee theft and the geographic location of the misused identities.
6. More organized misuse occurred with new application for bank credit cards than applications for new wireless phones or retail credit cards.

Discussion

For a copy of the “Data Breach Harm Analysis” White Paper, visit our website at www.idanalytics.com or email marketinginfo@idanalytics.com.

'id:analytics™