BerkeleyLaw
UNIVERSITY OF CALIFORNIA

BERKELEY CENTER FOR
LAW & TECHNOLOGY

Identity Theft: Shifting Focus from Criminals and Consumers to Businesses

Chris Jay Hoofnagle
Director, Information Privacy Programs

For The John Jay College of Criminal Justice
October 20, 2009

Thesis: identity theft as a business process problem

Overview of discussion

- Costs of identity theft
- How credit authentication works (and fails)
  - Negligent credit granting cases
  - Synthetic identity theft
- Two methods of addressing identity theft
  - FACTA Access
  - Measuring identity theft

Implications

- How should we allocate law enforcement resources?
- Should we adopt biometric or other more complex authentication systems to prevent identity theft?
- Should we adopt national identification to prevent identity theft?

What is identity theft?

Identity theft is the knowing use of identification information of another to commit any unlawful activity

- 18 USC §1028

A fraud committed or attempted using the identifying information of another person without authority

- 16 CFR § 603.2 (2006)

Criminal prosecutions low

Estimated that 1 in 700 identity thieves are arrested by federal authorities

Gartner Group

Anecdotal pickup

Two types of financial identity theft

Account takeovers (most identity theft)

Thief takes control of an existing account.

- 67% credit card
- 19% checking/savings
- 9% telephone service

New account fraud

Thief establishes new lines of credit using personal information from the victim

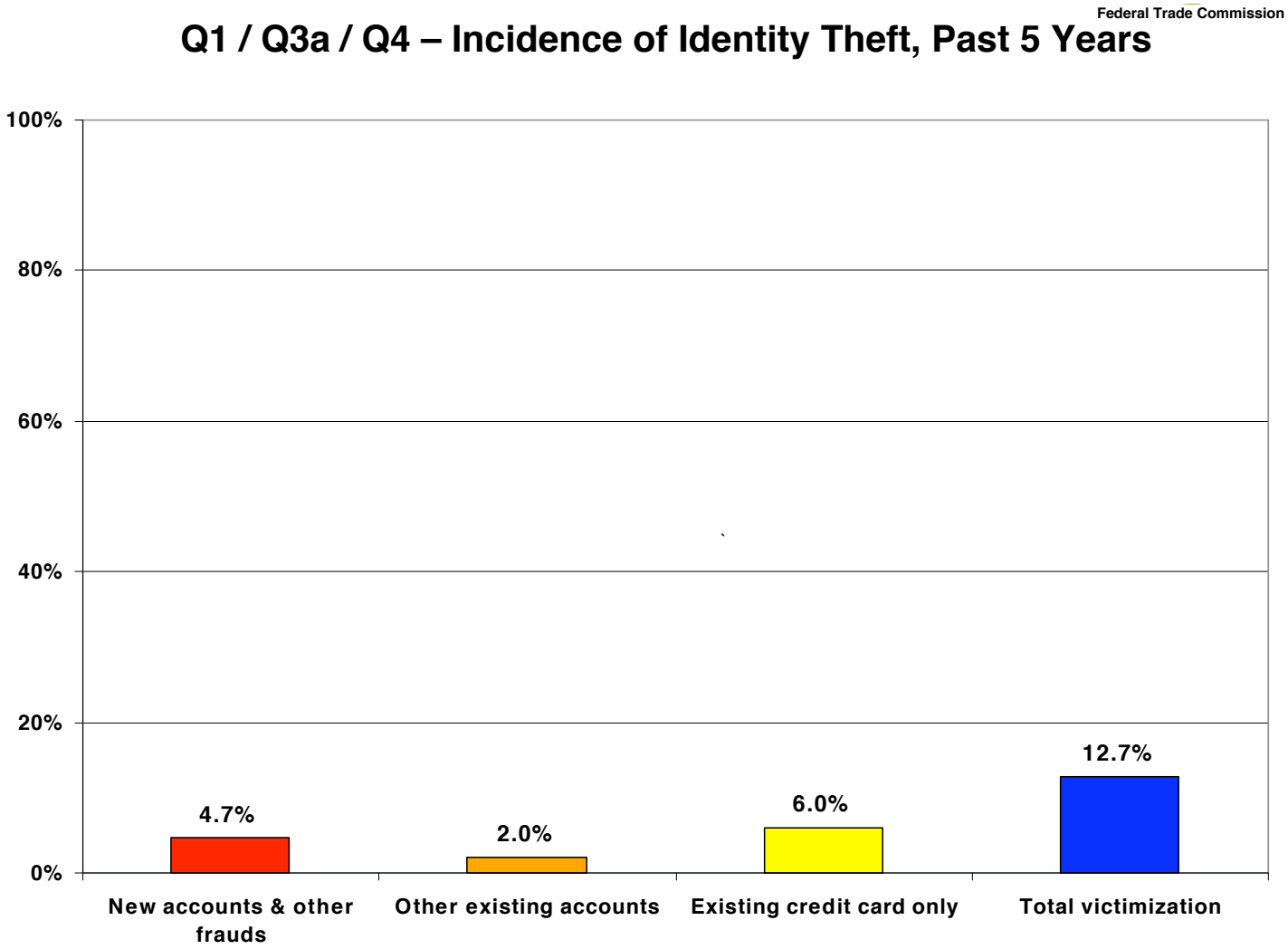
Synthetic fraud: mixture of real and false personal information

Other variations not addressed here

Criminal identity theft

Identity cloning

Account takeovers are more prevalent

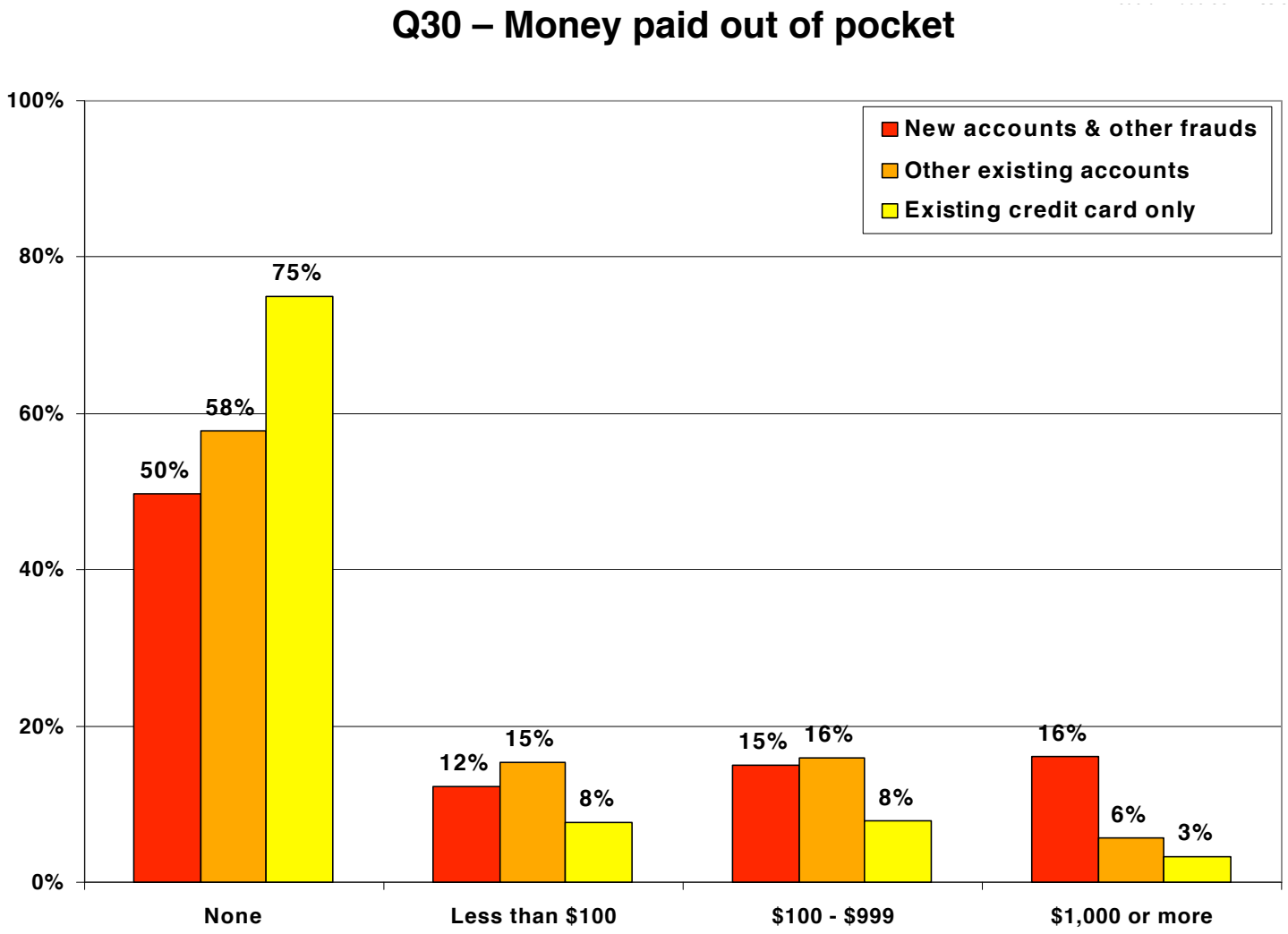


Source: FTC 2003 Report, Page 11

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

BERKELEY CENTER FOR LAW & TECHNOLOGY

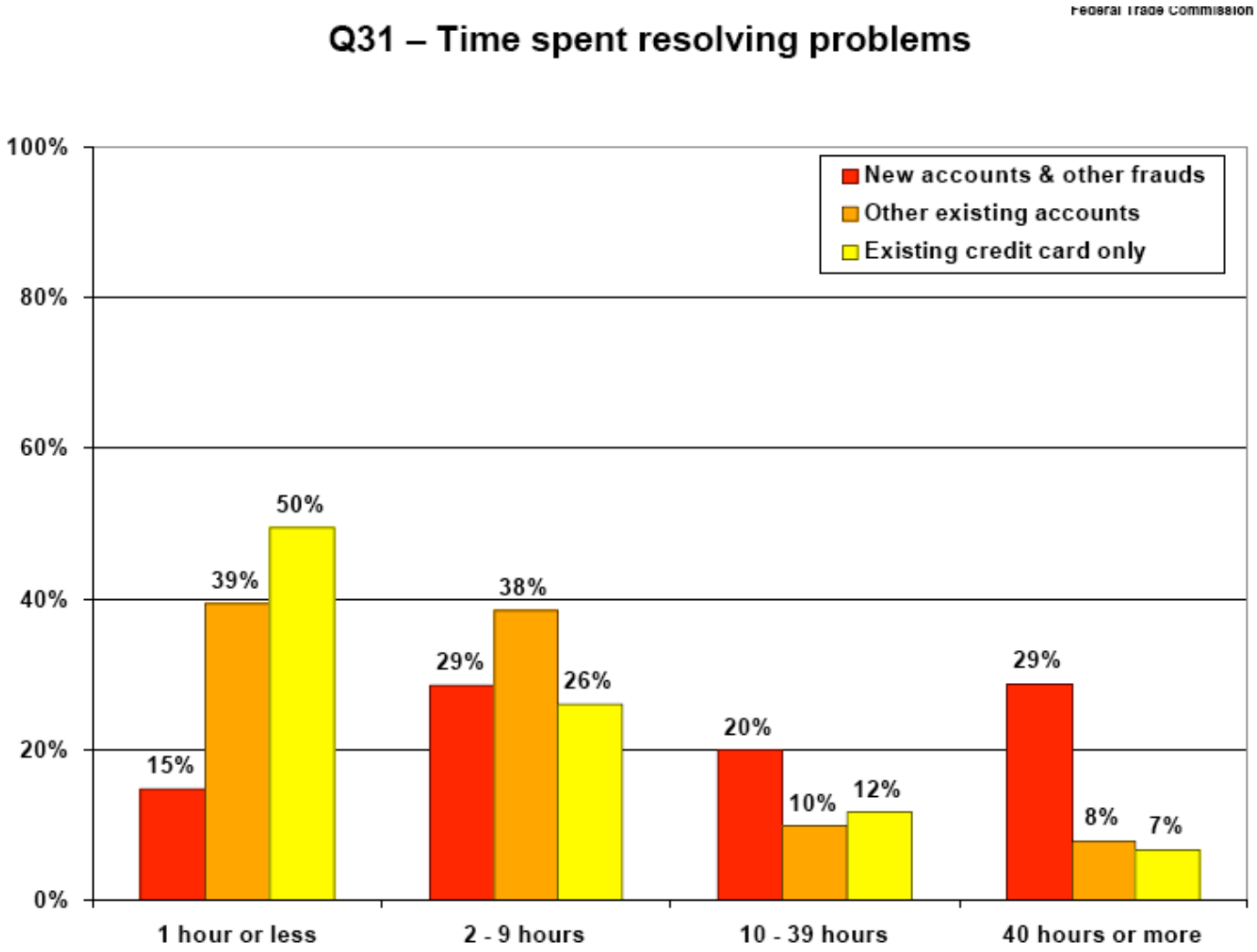
But new account fraud = higher costs to victims



Source: FTC 2003 Report, Page 43

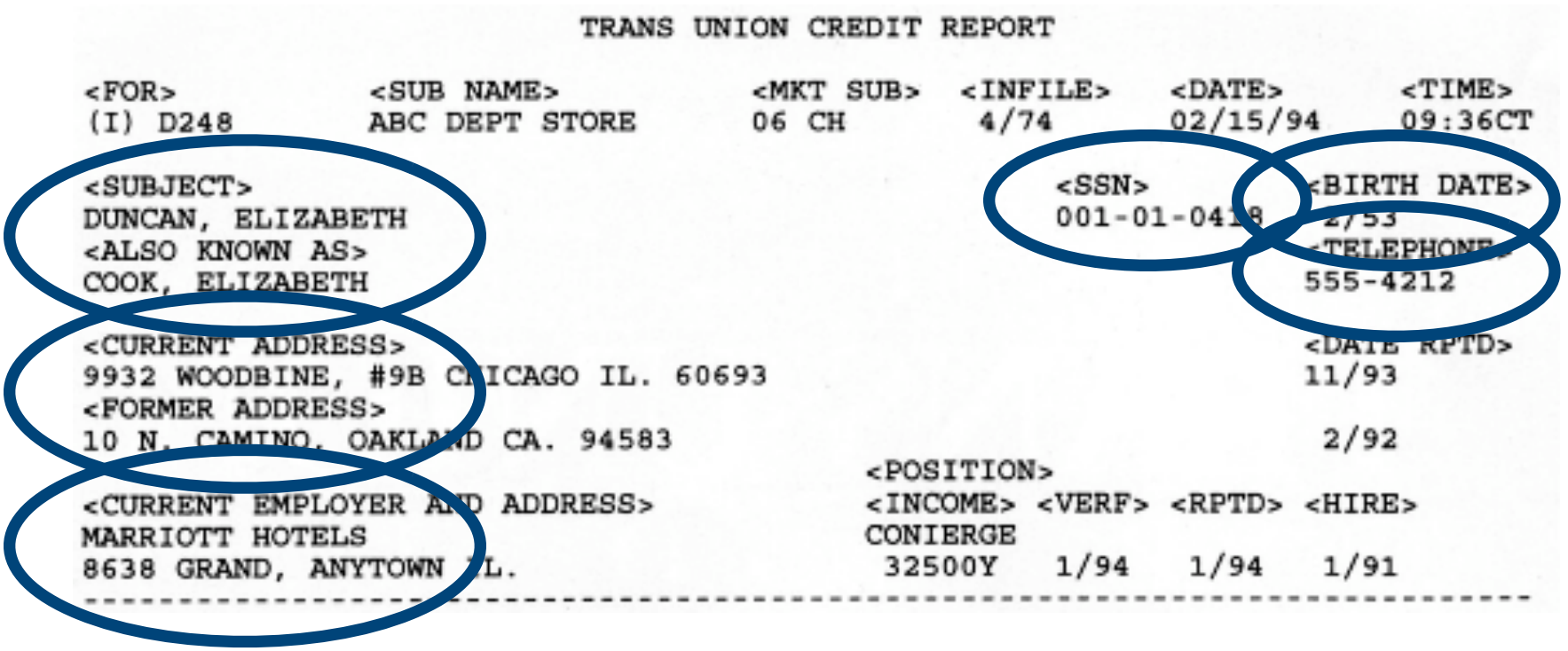
BerkeleyLaw UNIVERSITY OF CALIFORNIA | BERKELEY CENTER FOR LAW & TECHNOLOGY

And lost time



Source: FTC 2003 Report, Page 45

How credit authentication works



TRANS UNION CREDIT REPORT

<FOR>	<SUB NAME>	<MKT SUB>	<INFILE>	<DATE>	<TIME>
(I) D248	ABC DEPT STORE	06 CH	4/74	02/15/94	09:36CT

<SUBJECT>
DUNCAN, ELIZABETH
<ALSO KNOWN AS>
COOK, ELIZABETH

<SSN>
001-01-0418

<BIRTH DATE>
2/53

<TELEPHONE>
555-4212

<CURRENT ADDRESS>
9932 WOODBINE, #9B CHICAGO IL. 60693

<DATE RPTD>
11/93

<FORMER ADDRESS>
10 N. CAMINO, OAKLAND CA. 94583

2/92

<CURRENT EMPLOYER AND ADDRESS>
MARRIOTT HOTELS
8638 GRAND, ANYTOWN IL.

<POSITION>	<INCOME>	<VERF>	<RPTD>	<HIRE>
CONIERGE	32500Y	1/94	1/94	1/91

If there is no match...

The credit grantor might ask for more information to get a good match or ultimately reject the application

"No hit:" SSN doesn't match name, grantor may assume that the customer doesn't have a credit file at all

- Some creditors grant in no file situations

Credit granting and the law - business regulations

CRAs are required to "maintain reasonable procedures designed" to prevent unauthorized release of consumer information

- 15 U.S.C. § 1681e(a)

California: in in-store, instant credit situations, 3 identifiers must match.

- First and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number, but ~mother's maiden name
  - California Civil Code § 1785.14

"Red Flags" Rule

- Must identify "patterns, practices, and specific forms of activity" associated with identity theft
- Must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft

Credit granting and consumer self-help

A user-initiated fraud alert requires "reasonable policies and procedures to form a reasonable belief that the user [credit grantor] knows the identity of the person making the request."

- Usu. means call to cell phone or password
  - However, no contact w/ victim/impostor required
- No statutory penalty for ignoring the alert
  - ITRC finds 19% of cases fraud alert is ignored

Credit Freeze requires the consumer to contact the CRA and "thaw" the report, otherwise the credit grantor cannot obtain the report, and therefore, cannot grant credit

How credit auth. fails (the negligent granting cases)

Matching SSN, but incorrect DOB, address thousands of miles away from the victim

- Vazquez-Garcia v. Trans Union De P.R., Inc., 222 F. Supp. 2d 150 (D. Puerto Rico 2002)

6 AMEX cards obtained using matching name and SSN, but all sent to the impostors' home

- United States v. Peyton, 353 F.3d 1080 (9th Cir. 2003)

Bank issued two credit cards based on matching name and SSN but incorrect address

- Aylward v. Fleet Bank, 122 F.3d 616 (8th Cir. 1997)

Matching SSN but incorrect address

- Dimezza v. First USA Bank, Inc., 103 F. Supp. 2d 1296 (D.N.M. 2000)

Wolfe v MBNA, 485 F. Supp. 2d 874 (WD. Tenn. 2007)

MBNA telemarketer approves application with false address, phone #, relative.

- 21 year old student applicant with no job
- Application claimed $55k income
- MBNA: "Nothing was verified."
  - –(Plaintiff's Response in Opposition to Defendant MBNA's Motion to Dismiss Fourth Amended Complaint)

Court: case against MBNA may proceed on negligence! MBNA settles the case!

SSN Only Fraud?

"Making purchases on credit using your own name and someone else's Social Security number may sound difficult…But investigators say it is happening with alarming frequency because businesses granting credit do little to ensure names and Social Security numbers match and credit bureaus allow perpetrators to establish credit files using other people's Social Security numbers."

- Lesley Mitchell, *New wrinkle in ID theft;Thieves pair your SS number with their name, buy with credit, never get caught; Social Security numbers a new tool for thieves*, The Salt Lake Tribune, June 6, 2004, at E1

Synthetic identity theft

18. Beginning on or about February of 2001 to on or about May of 2003, in the State and District of Arizona and elsewhere, the defendant, JAMES J. ROSE and others known and unknown to the Grand Jury, devised and intended to devise a scheme and artifice to defraud at least 15 financial institutions issuing credit cards and obtain money in excess of $760,000.00 by means of false and fraudulent pretenses and representations.

US v. Rose et al, CR06-0787PHK-JAT (VAM) (D.Az. 2006), indictment filed Aug. 22, 2006.

Real SSN, fake name, real address = synthetic person

Count	Date (on or about)	False Name	Amount of money obtained from use	Credit card #
1	05/02/2002	Hanna Curin (SSN 7483 assigned to Haqqani Saifullah)	$3,481.00	Fleet #0519
2	05/02/2002	Danni Curin (SSN 1969 assigned to Polly Hatch	$4,981.00	HHB #5179
3	05/02/2002	Adam Gregory (Las Vegas) (SSN 9855 assigned to Mary Harry	$4,983.00	HHB #0141
4	05/24/2002	A.J. Rose (Seattle) (SSN 4487, assigned to Mehdi Sonboli)	$3,486.00	Fleet #3988
5	05/28/2002	Jamei Enrico (SSN 3707 assigned to Manuel Hernandez	$2,984.00	Nova #4595

How does synthetic identity theft work?

Thieves know SSN structure

- 111-22-1234
  - –555 (area number, geographically linked)
  - –22 (group numbers, linked to issuance date)
  - –1234 (serial number, unique)

Thesis: identity theft is a business process problem

The negligent credit granting cases show that new accounts can be obtained with obvious errors on the application

The synthetic cases show that only the SSN and DOB need to be linked for credit granting

My hypothesis: Some credit grantors are authenticating applicants by "verifying" the SSN (matching the group number with date of birth).

Testing the hypothesis: FACTA Access Study

The FACTA (Fair and Accurate Credit Transactions Act of 2003) allows victims of identity theft to obtain business records associated with the crime from the company that created an account for the impostor in the victim's name

The goal of the FACTA Access Study is to discover the human factors and decision making at businesses that have opened accounts to impostors. Through obtaining the business records in identity theft cases, we will be able to evaluate both business practices and defenses to identity theft

Measuring identity theft

Parallels with motor vehicle safety

Can a market for preventing identity theft can be fostered among lending institutions?

Draws upon several sources of data

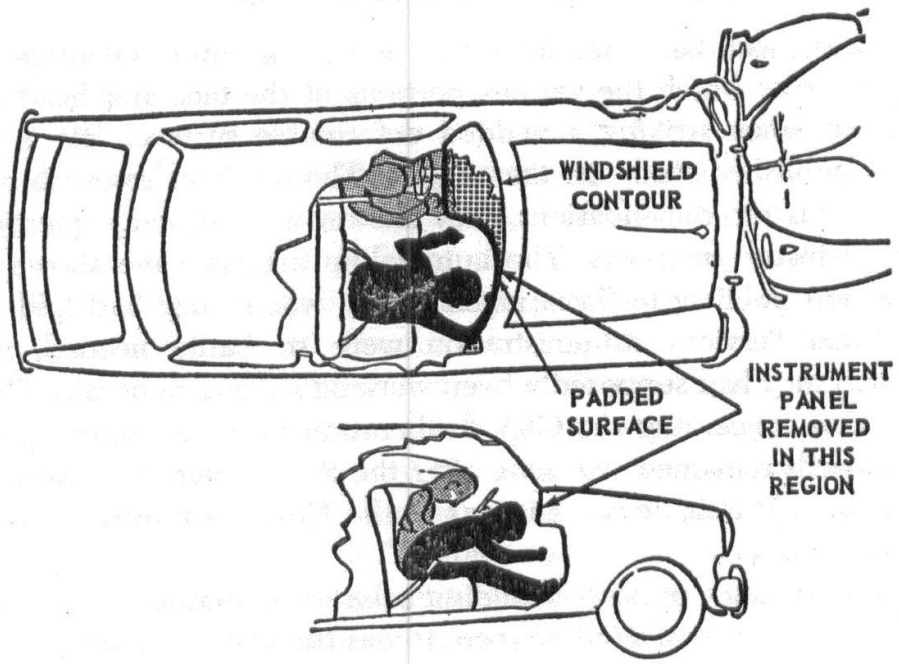
- FTC consumer complaint data
- FDIC bank statistics
- Proprietary ranking statistics

Auto safety...not that long ago...

It's the driver's fault, ∴

- Focus should be on "driver education"
- Significant underinvestment in safety
- Dialogue suffered from a lack of data and understanding of accident physics

FIGURE 5



ELIMINATION OF INSTRUMENT PANEL AT RIGHT FRONT POSITION

Auto safety: now

It's the driver's fault, **but**

- Testing, ratings available
- Data drives inclusion of new accident mitigation, avoidance technology
- A market for safety has emerged, with once top-of-the-line features appearing in inexpensive cars

Federal Trade Commission consumer victim data

6. Companies

Please identify companies or organizations where fraudulent accounts were established or your current accounts were affected. Please provide as r
or activity as possible.

Company 1

Company Name:

Type of Account:

New Account? ○ Yes ○ No

Date Issued or Misused: **(MM/DD/YYYY)**

Amount Thief Obtained ($):
(Numbers Only)

Credit Limit ($):
(Numbers Only)

Contact Person:

Contact Phone: **Ext.**
(Area Code)(Phone Number)(Extension)

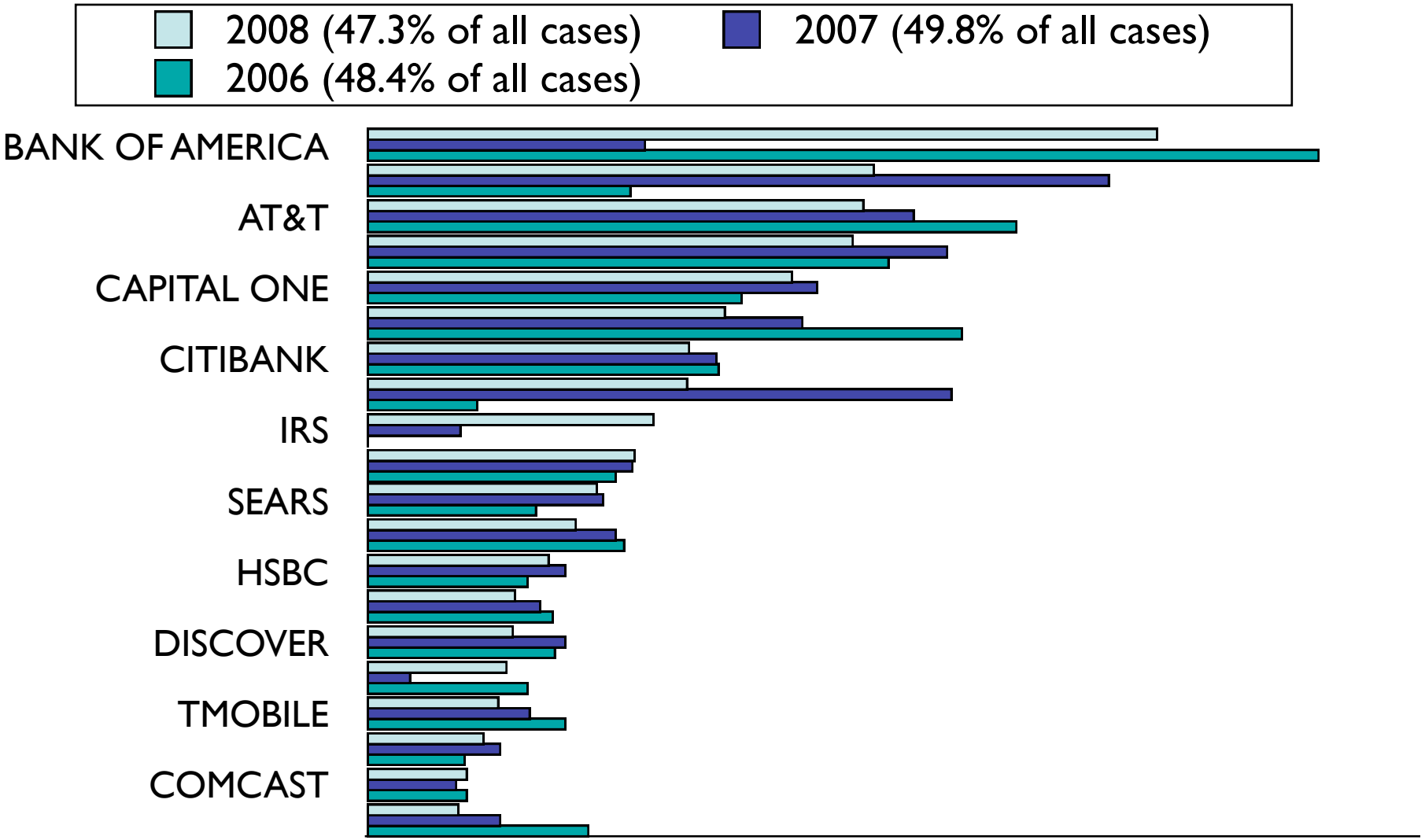
Have you notified this company? ○ Yes ○ No

Have you sent written notifications to this company? ○ Yes ○ No

Methods challenges

- 150k complaints aggregated over three years
  - About 275k reported a year
- No data on takeovers vs. new account
  - FTC database limitations
- Underreporting
  - Only 1 in ~32 victims file a report with the FTC
- Misidentification
  - e.g. AT&T
  - Retailer cases may be new account or takeover situations
- Some banks forward complaints to the FTC automatically

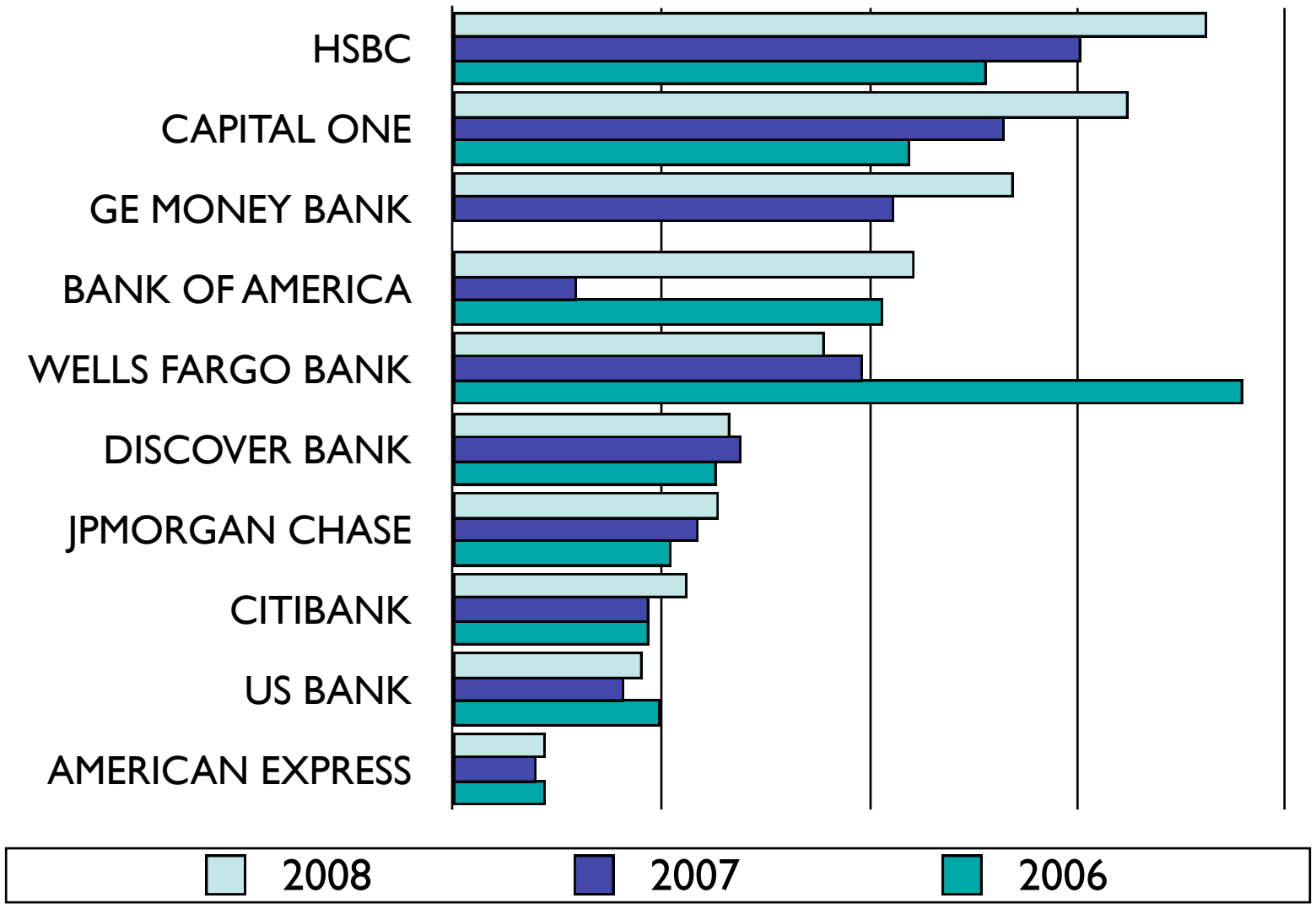
25 companies account for about 50% of incidents



BerkeleyLaw
UNIVERSITY OF CALIFORNIA

BERKELEY CENTER FOR
LAW & TECHNOLOGY

Meaningful rates are difficult to create w/ current data



BerkeleyLaw
UNIVERSITY OF CALIFORNIA

BERKELEY CENTER FOR
LAW & TECHNOLOGY

Policy implications

- Identity theft is a cost of doing business
  - But externalities are imposed on the public
  - Might look to tax policy to address the externalities
- Loose authentication practices = opportunities for improvement without law enforcement resources
  - Red flag rules
  - Targeted education to top 25 list
  - Frees law enforcement resources for more intractable frauds
- Biometric/National identification?
  - Authentication problems still need to be fixed

Questions?

Chris Hoofnagle
choofnagle@law.berkeley.edu
510.643.0213