DETER·DETECT·DEFEND

AVOID THEFT

www.ftc.gov/idtheft

Avoid ID Theft

How to Deter, Detect, and Defend Against Identity Theft

Bruce E. Sullivan

Visa, U.S.A.

THE FEDERAL TRADE COMMISSION

VISA

Breach exposes 4.2 million credit, debit cards

Another Month, Another massive Credit Card Breach

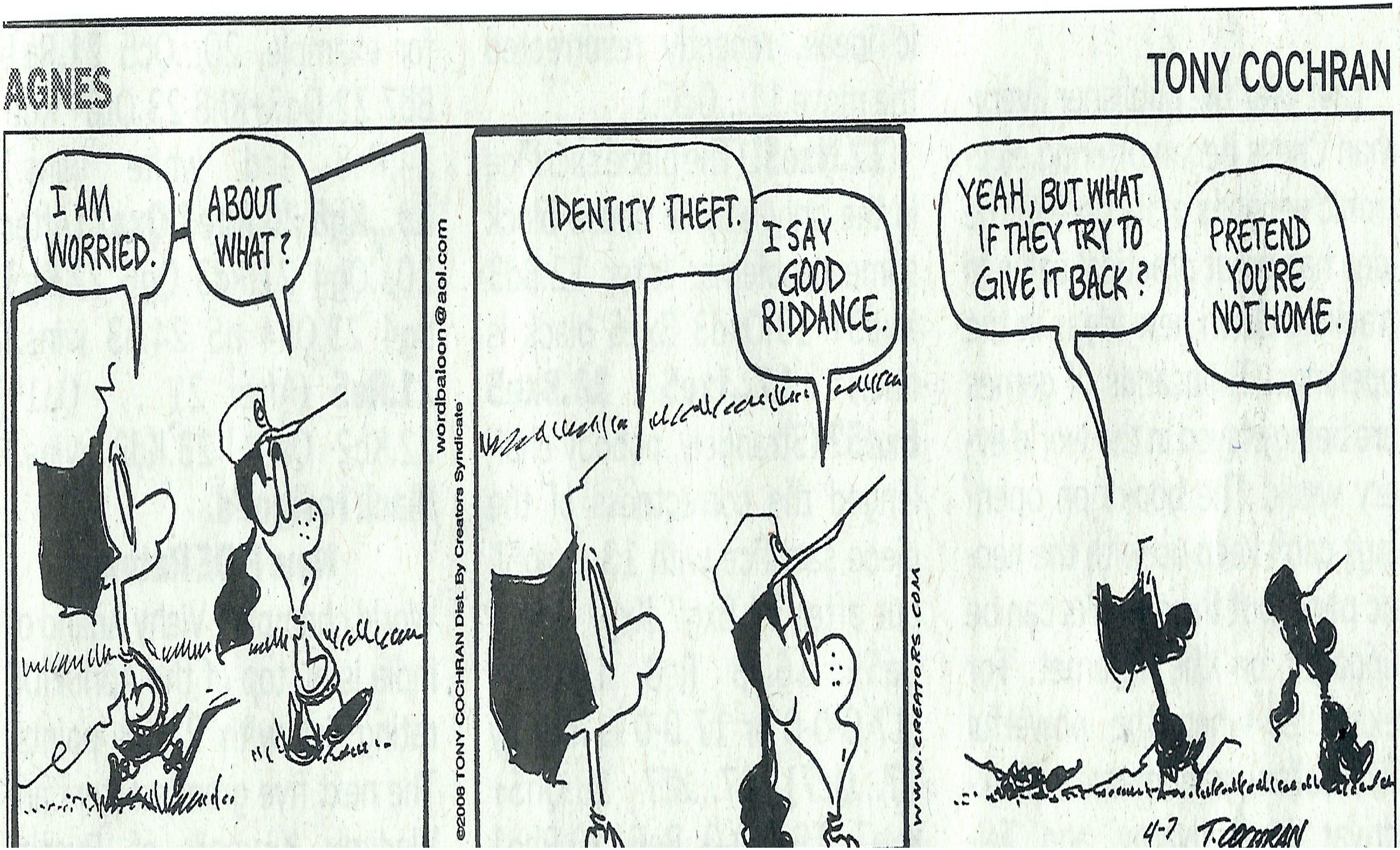
TSP Hacked

USAF Personnel System Hacked

Escaped the largest credit card data breach ever?

Well here's another one...

Workers stealing company data


AGNES
TONY COCHRAN
I AM WORRIED.
ABOUT WHAT?
©2008 TONY COCHRAN Dist. By Creators Syndicate
wordbaloon@aol.com
IDENTITY THEFT.
I SAY GOOD RIDDANCE.
WWW.CREATORS.COM
YEAH, BUT WHAT IF THEY TRY TO GIVE IT BACK?
PRETEND YOU'RE NOT HOME.
4-7 T.COCHRAN

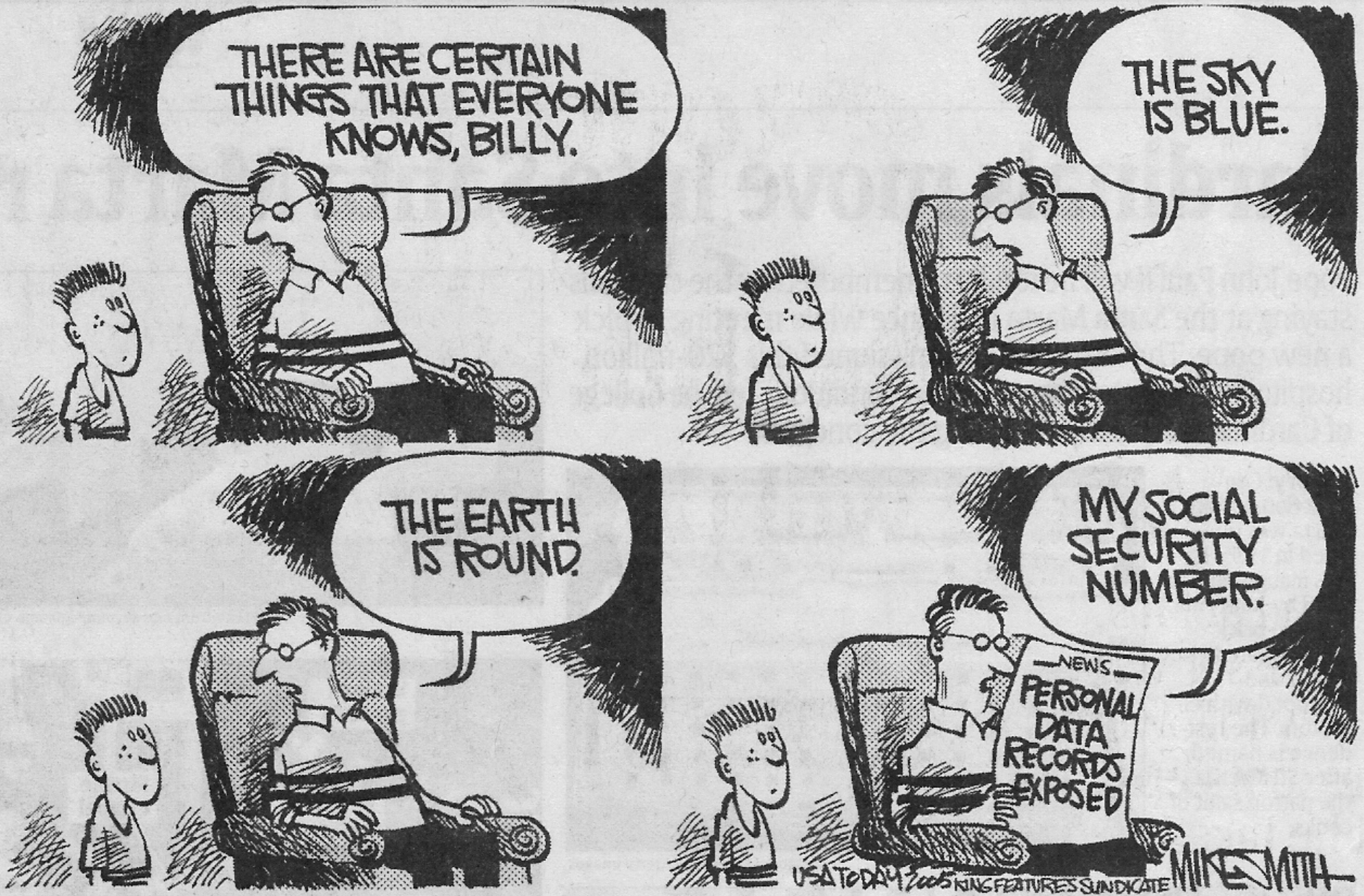
Identity Theft

9.9 Million Americans (increase of 25%)
$48 Billion in losses (increase of 7%)
$4,849 average loss (down by 12%)
30 hours of your time to resolve (increase of 15%)
43% caused by lost wallet, checkbook, cards
13% of victims identified friends, family, employees as perpetrator (50% of theft where victims knew who).

2009 Identity Fraud Survey Report, Javelin Strategy & Research, February 2009

what is identity theft?

- It occurs when someone steals your personal information e.g., credit card or Social Security number – and uses it fraudulently
- It can cost you time and money
- It can destroy your credit and ruin your good name


THERE ARE CERTAIN THINGS THAT EVERYONE KNOWS, BILLY.
THE SKY IS BLUE.
THE EARTH IS ROUND.
MY SOCIAL SECURITY NUMBER.
NEWS
PERSONAL DATA RECORDS EXPOSED
USA TODAY ©2005 KING FEATURES SYNDICATE
MIKE SMITH

By Mike Smith, *Las Vegas Sun*, for USA TODAY

Letters

What can you do?

DETER

- Deter identity thieves by safeguarding your information

DETECT

- Detect suspicious activity by routinely monitoring your financial accounts and billing statements

DEFEND

- Defend against identity theft as soon as you suspect a problem

Where do thieves get your information?

Identity thieves may:

- Go through your trash or “dumpster dive”
- Steal your wallet or purse
- Steal your mail and/or submit a change of address form for your mail

Where do thieves get your information?

Identity thieves may:

- Steal personnel records from their employers
- Obtain personal information from your computer
- Use “phishing” or fake emails to get you to provide personal information

Use “phishing” or virus’ to get your personal information

Spam volumes rose strongly in 2008 and TRACE estimates that global spam volume exceeded 150 billion messages per day at its peak.

Blended attack spam which directs users to Web pages hosting malicious code via URL links rose strongly in mid-2008, peaking at 33% of all spam. However, this dropped to a more typical level of 1% by the end of the year.

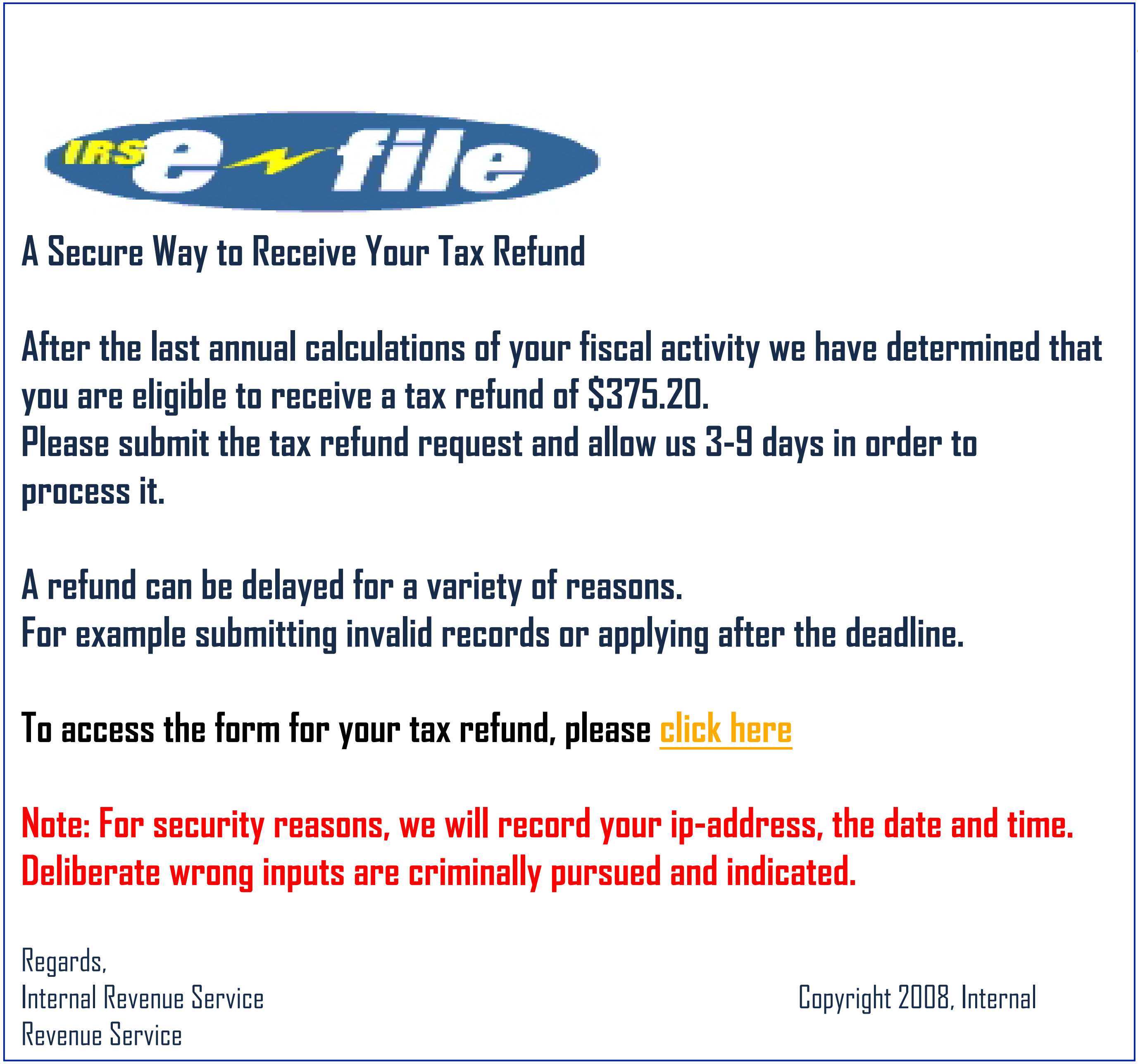
Phishing volume rose in 2008 peaking at nearly 4%of all spam, however, phishing has declined to less than 1%.

Browser vulnerabilities continued to be a key attack vector for criminals.

Literally millions of legitimate Websites are now hosting malicious code. Mass Website attacks by botnets are one of the most concerning developments of 2008.

The social networking sites MySpace, Facebook, Bebo, and others came under attack by malware called Koobface that spread links to other users in an effort to distribute malware.

Marshal8e6 Security Threats: Email and Web Threats
By Marshal8e6 TRACELabs January 2009



A Secure Way to Receive Your Tax Refund

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of $375.20.
Please submit the tax refund request and allow us 3-9 days in order to process it.

A refund can be delayed for a variety of reasons.
For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here

Note: For security reasons, we will record your ip-address, the date and time.
Deliberate wrong inputs are criminally pursued and indicated.

Regards,
Internal Revenue Service
Revenue Service

Copyright 2008, Internal

Internal Revenue Service [forms@irs.fe.com]

Beware of emails

Fake Microsoft Security Update

October 13, 2008

Malicious Emails being sent from the Pushdo botnet are pretending to be Microsoft Windows updates. The emails appear to come from customerservice@microsoft.com and contain an attachment named KBXXXXXX.exe, where X is a random number. This is a similar naming convention to many legitimate Microsoft updates.

To add to the legitimacy of the email the message contains a PGP signature at the end.

MARSHAL

Secure. Protect. Comply.

Beware of emails

Malicious Spam Using Dramatic Subjects to Lure Users

July 7, 2008

Over the weekend we have seen an increase in the number of spam emails with dramatic subject lines. They contain a link to the file r.html hosted on several compromised websites. Some of the subject lines seen today are:

Incredible Hulk premiere highlights

Homeless man wins lottery

Clinton says: Hiliray cheated on me

Olsen twins caught nude on camera

Playboy party invite

Man goes berserk in office

Brad Pitt strips naked for Playgirl

Video of rampage in Tokyo

Angelina Jolie dies in plane crash

Plane crashed into White House, injuring hundreds

Clicking on the link in one of these emails will take you to a malicious 'PornTube' website that contains malware and hidden IFrames.

It is important that recipients of these emails not open them or click on links inside them. Many website hosting malware also contain scripts or IFrames hosted on other sites that can exploit vulnerabilities in browsers and plugins to install malware without the users knowledge.

MARSHAL®
Secure. Protect. Comply.

Is it Phishing?

1. Does the email ask you to go to a website and verify personal information? Banks won't ask you to verify your personal information in response to an email.

2. What is the tone of the mail? Most phish emails convey a sense of urgency by threatening discontinued service or information loss if you don't take immediate action.

3. What is the quality of the email? Many phish emails have misspellings, bad grammar, or poor punctuation.

4. Are the links in the email valid? Deceptive links in phishing emails look like they are to a valid site, but deliver you to a fraudulent one. Many times you can see if the link is legitimate by just moving your mouse over the link.

5. Is the email personalized with your name and applicable account information? Many phish emails use generic salutations and generic information (e.g. Dear Customer or Dear Account Holder) instead of your name.

6. What is the sender's email address? Many phish emails come from an email address not from the company represented in the email.

7. When in doubt, type it out. If you suspect an email to be phishing, don't click on any links in the email. Type the valid address directly into your web browser.

Where do thieves get your information?

Identity thieves may:

- They get your information from the businesses in a practice known as “business record theft” (customer, employee, patient or student; bribing an employee who has access to your files; or “hacking” into electronic files).

Where do thieves get your information?

Data Breaches **Up Almost 50 Percent**, Affecting Records of **35.7 Million People**

The Washington Post, January 06, 2009 (US) -- Businesses, governments and educational institutions reported nearly 50 percent more data breaches last year than in 2007, exposing the personal records of at least 35.7 million Americans, according to a nonprofit group that works to prevent identity fraud. Identity Theft Resource Center of San Diego is set to announce today that some **656 breaches were reported in 2008**, up from 446 in the previous year. Nearly 37 percent of the breaches occurred at businesses, while schools accounted for roughly 20 percent of the reported incidents. The center also found that the percentage of breaches attributed to data theft from current and former employees more than doubled from 7 percent in 2007 to nearly 16 percent in 2008. "This may be reflective of the economy, or the fact that there are more organized crime rings going after company information using insiders," said Linda Foley, the center's co-founder. "As companies become more stringent with protecting against hackers, insider theft is becoming more prevalent."

They get your information from the businesses… “hacking” into electronic files.

VISA

10TH ANNIVERSARY
GOVEXEC.COM

DAILY BRIEFING
May 1, 2006

Hackers access personal information on TRICARE servers

By Daniel Pulliam
dpulliam@govexec.com

Hackers gained access to the Pentagon's health insurance information systems, compromising the personal information of more than 14,000 people…

The intrusion of the TRICARE Management Activity public computer servers was discovered on April 5...The hacked information included databases of names, Social Security numbers, the last four digits of credit card numbers, personal phone numbers, work and personal e-mail addresses and home addresses.

The Defense Criminal Investigative Service is participating in an investigation of the incident.

The department sent affected people letters informing them that the compromise of their personal information could put them at risk for identity theft and recommending precautionary measures.

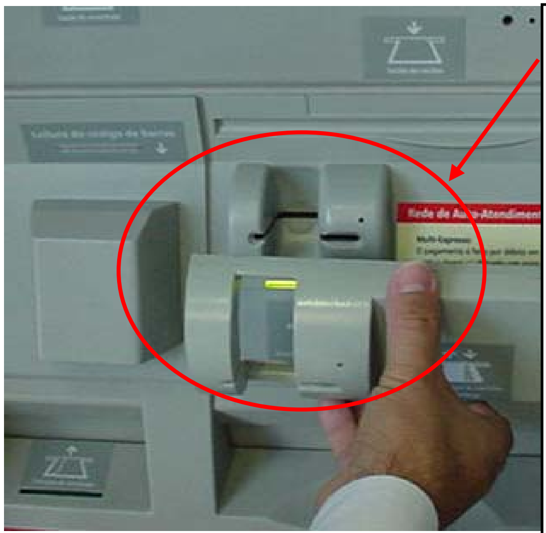
"A security problem of this magnitude on this level underscores the need to address security as a fundamental issue on the development and implementation of any national electronic health care record initiative," McNulty said.

They get your information from the businesses…
“hacking” into electronic files.

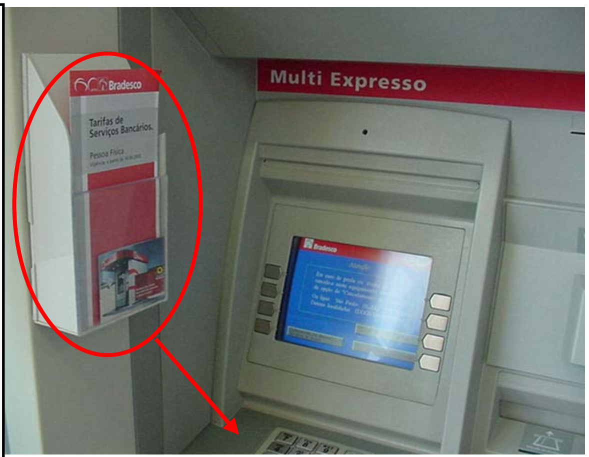
Data Breaches Cost Businesses More
The Wall Street Journal (US) Tuesday, February 03, 2009 --

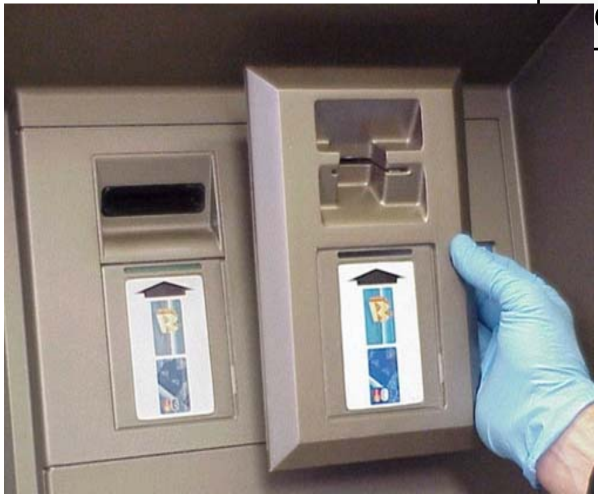
Losses of confidential data, similar to those that occurred recently at credit-card processor Heartland Payment Systems Inc., are costing businesses more. In an annual survey released February 9th, data-privacy research firm Ponemon Institute found that the cost of a data breach rose to $202 for each compromised record last year, an increase of 2.5 percent over 2007. That average expense to an organization was $6.6 million in direct and indirect costs, which includes the cost of notifying victims and maintaining information hot lines as well as legal, investigative and administrative expenses. Health-care and financial-services companies lost the most customers after data breaches, as customers most expect these companies to protect their privacy. The average cost of a health-care breach was $282 per record, while the cost of the average retail breach was $131. Financial-services firms' costs don't include actual financial costs absorbed by the banks in credit-card fraud and account takeover, said Larry Ponemon, chairman and founder of the Ponemon Institute. Dr. Ponemon said the vast majority of data breaches were caused by negligence and that portable storage devices, including laptops, are responsible for a growing number of breaches.

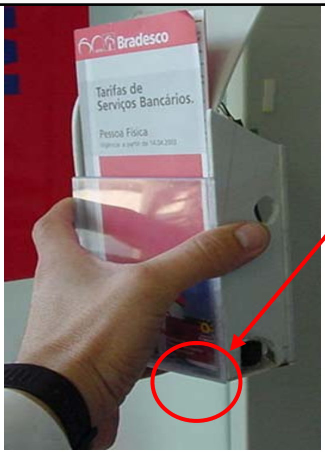
They skim or otherwise obtain your card information

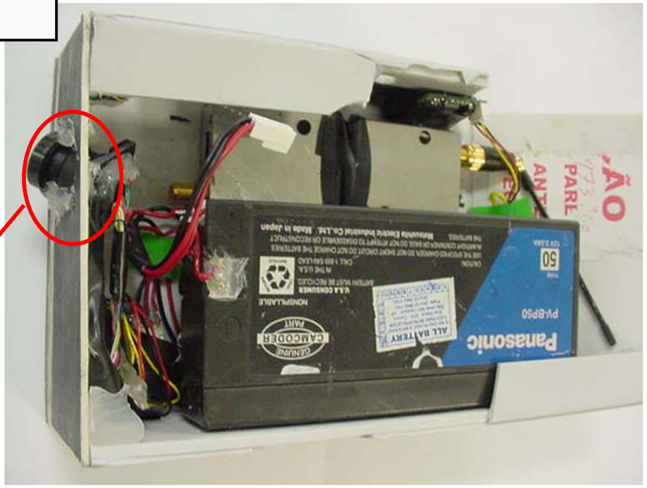


- False fronts on ATM terminals with built in magnetic stripe readers.
- Hidden camera captures PIN and transmits the information to a nearby crook
- Increasingly common

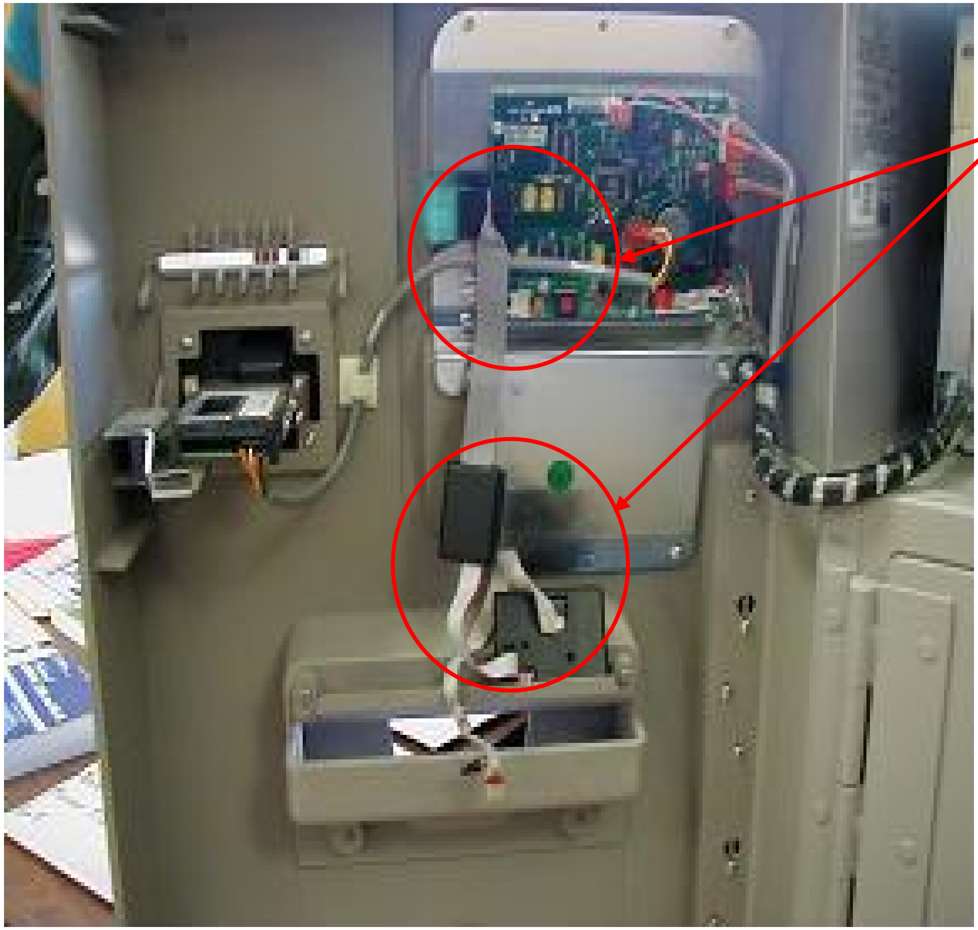








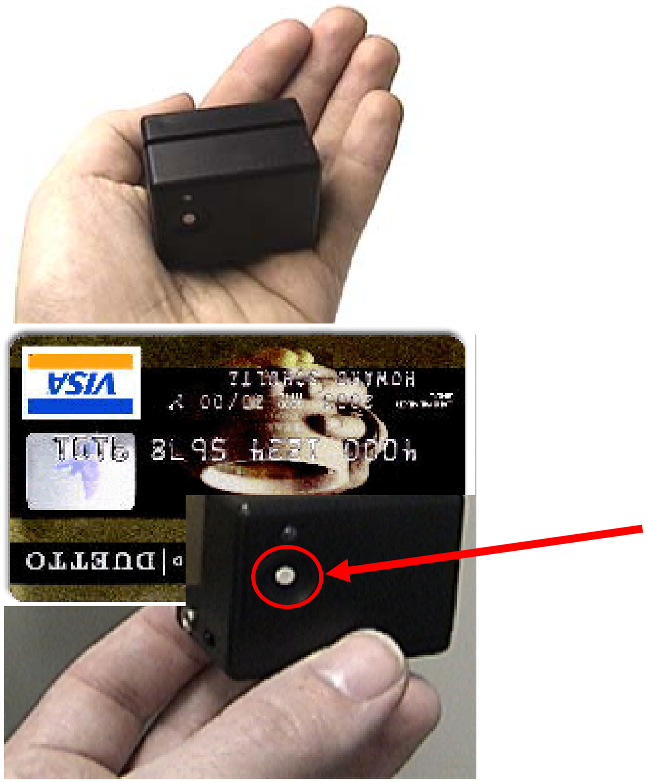
ATM – Environment – Cont'd



- Sniffing devices installed in ATMs are another example of how a fraudster can compromise the ATM or Debit card PIN. In this example, the PIN and magnetic stripe information are captured before encryption.

- Recent cases have Bluetooth transmission to remote receiver.

And An Old Favorite – "The Skimmer"



This device can capture over 2500 credit card account numbers, expiration dates and CVV codes in the palm of your hand.

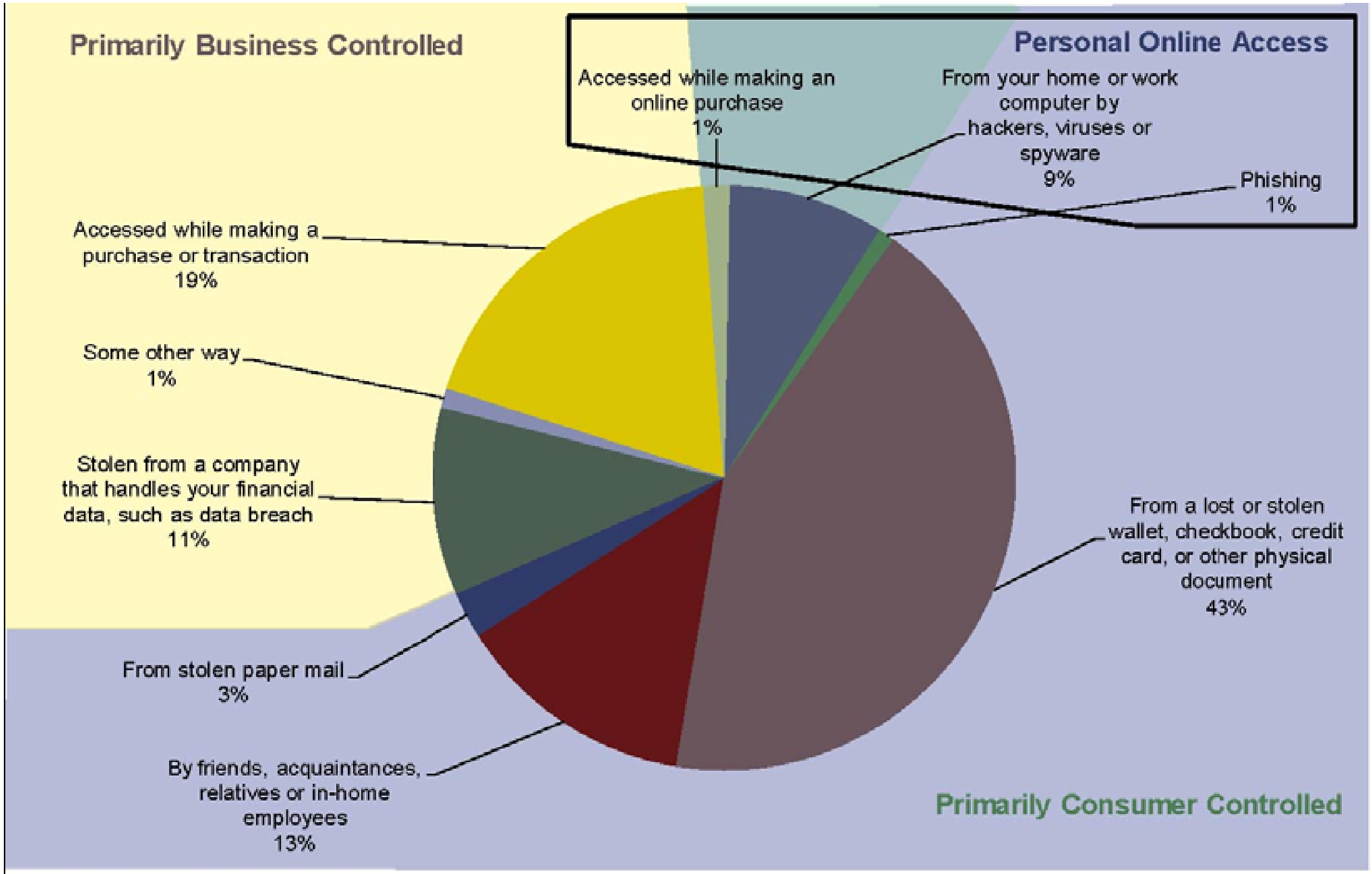
The unit can operate continuously for 40 hours on a single 3V battery (6000 swipes).

Skimmed data can be downloaded to any PC with software provided.

At a moment's notice, or the moment of arrest, the contents can be deleted with the press of a button to avoid prosecution.

Cost = $500

Offline Versus Online Methods of Access Causes Of Known Theft



Q28: How was your information obtained? Keep in mind 'other' is an option. Was it obtained...

October 2008, n = 157
(Based on the 35% of Victims Who Know How Their Information Was Obtained)
Base: Victims Who Know How Their Information Was Accessed.
© 2009 Javelin Strategy & Research

DETER identity thieves by safeguarding your information.

- Shred financial documents before discarding them
- Protect your Social Security number
- Don’t give out personal information unless you’re sure who you’re dealing with

DETER identity thieves by safeguarding your information.

- Don’t use obvious passwords
- Keep your information secure
- Use a Firewall, Virus Protection, Anti-Spyware Software
- Carry only the identification information and credit and debit cards that you’ll actually need.

To Freeze or not to Freeze

What is a credit freeze?

Many states have laws that let consumers "freeze" their credit – in other words, letting a consumer *restrict access to his or her credit report*. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. This means that it's unlikely that an identity thief would be able to open a new account in your name. Placing a credit freeze does not affect your credit score – nor does it keep you from getting your free annual credit reports, or from buying your credit report or score.

Credit freeze laws vary from state to state. In some states, anyone can freeze their credit file, while in other states, only identity theft victims can. The cost of placing, temporarily lifting, and removing a credit freeze also varies. Many states make credit freezes free for identity theft victims, while other consumers pay a fee – typically $10. It's also important to know that these costs are for each of the credit reporting agencies. If you want to freeze your credit, it would mean placing the freeze with each of three credit reporting agencies, and paying the fee to each one.

District of Columbia (security freeze rights established by D.C. law)
Eligibility: All consumers
Fees: No fees for identity theft victims. All others pay $10 to place the freeze, but no fees to lift it temporarily, or remove it altogether. Effective date of law: July 1, 2007
Permanent freeze remains until removal requested by consumer.

Maryland (security freeze rights established by state law)
Eligibility: All consumers
Fees: No fees for identity theft victims who provide report of alleged identity fraud or with an identity theft passport. All others pay $5 to place the freeze, lift it temporarily, or remove it altogether. Effective date of law: January 1, 2008
Permanent freeze remains until removal requested by consumer.

On November 1, 2007, the security freeze was offered voluntarily by credit bureaus to consumers living in Alabama, Alaska, Arizona, Georgia, Idaho, Iowa, Michigan, Missouri, Ohio, South Carolina, and Virginia).

Are you Safe?
Take the Test!

www.idsafety.net

DETECT suspicious activity by routinely monitoring your financial accounts/billing Statements…and credit reports.

- Account take-over
  - Compromise of existing account information

- Establishing new accounts
  - Use of your personal information to open new accounts

DETECT suspicious activity by routinely monitoring your financial accounts/billing Statements…and credit reports.

- Be alert
  - Mail or bills that don’t arrive
  - Denials of credit for no reason
- Inspect your financial statements
  - Look for charges you didn’t make

DETECT suspicious activity by routinely monitoring your financial accounts/billing Statements…and credit reports.

- Inspect your credit report
  - Law entitles you to one free report a year from each Nationwide credit reporting agencies if you ask for it

    Online: www.AnnualCreditReport.com;

    by phone: 1-877-322-8228;

    or by mail: Annual Credit Report Request Service,
    P.O. Box 105281, Atlanta, GA 30348-5281

DEFEND against identity theft as soon as you suspect a problem.

- Contact Fraud Department of Creditors.
- Review reports carefully, looking for fraudulent activity
- Close accounts that have been tampered with or opened fraudulently
- File a police report
- Place a “Fraud Alert” on your credit reports
- Contact the Federal Trade Commission

WHERE CAN YOU LEARN MORE?

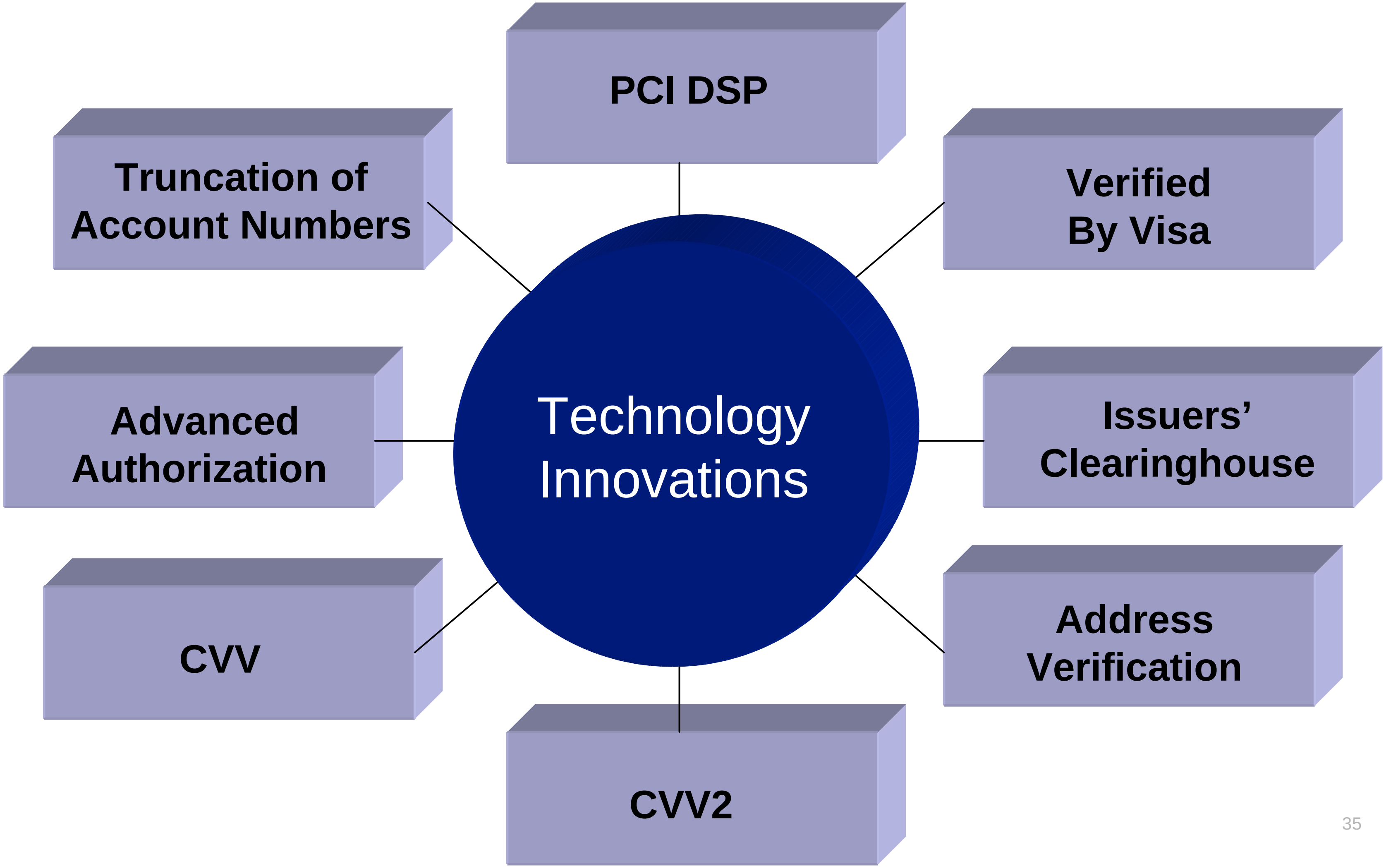
Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580 ftc.gov/idtheft

2009 Identity Fraud Survey Report:
Consumer Version
Prevent – Detect – Resolve
February 2009

Are you a Victim?
Professional help available!

1-866-ID-HOTLINE, victims can receive free and confidential assistance from trained counselors.

What's Visa doing?
Card Technological Safeguards



Technology Innovations

PCI DSP

Truncation of Account Numbers

Verified By Visa

Advanced Authorization

Issuers' Clearinghouse

CVV

Address Verification

CVV2