



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

July 1, 2015



ISOAG July 1, 2015 Agenda

- | | |
|--|---|
| I. Welcome & Opening Remarks | Michael Watson, VITA |
| II. State Level Computer Security Issues and Enforcement | Tommy Johnstone, Attorney Generals Office |
| III. Virtual Currency: System Overview and Threat Analysis | Jeremy D'Errico, FBI |
| IV. Upcoming Events | Bob Baskette/Michael Watson, VITA |
| V. Partner/Operation Update | Bob Baskette, VITA, Michael Clark, NG |



Welcome and Opening Remarks

Michael Watson

July 1, 2015



Virginia Information Technologies Agency

State-Level Computer Security Issues and Enforcement

Tommy Johnstone, Attorney Generals Office

July 1, 2015

State-Level Computer Security Issues and Enforcement



Tommy Johnstone

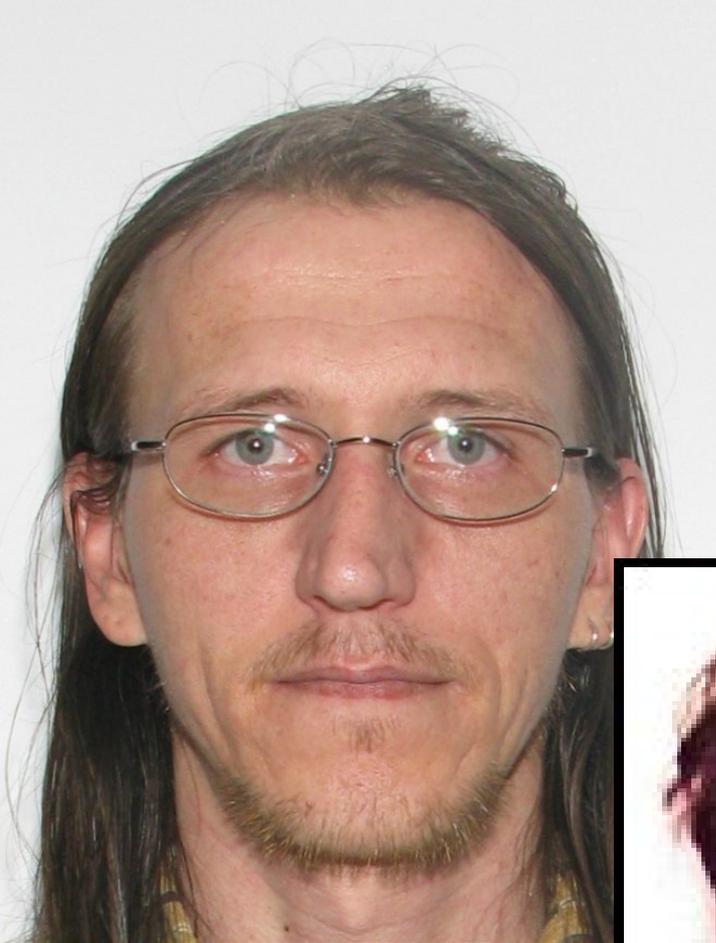
Assistant Attorney General

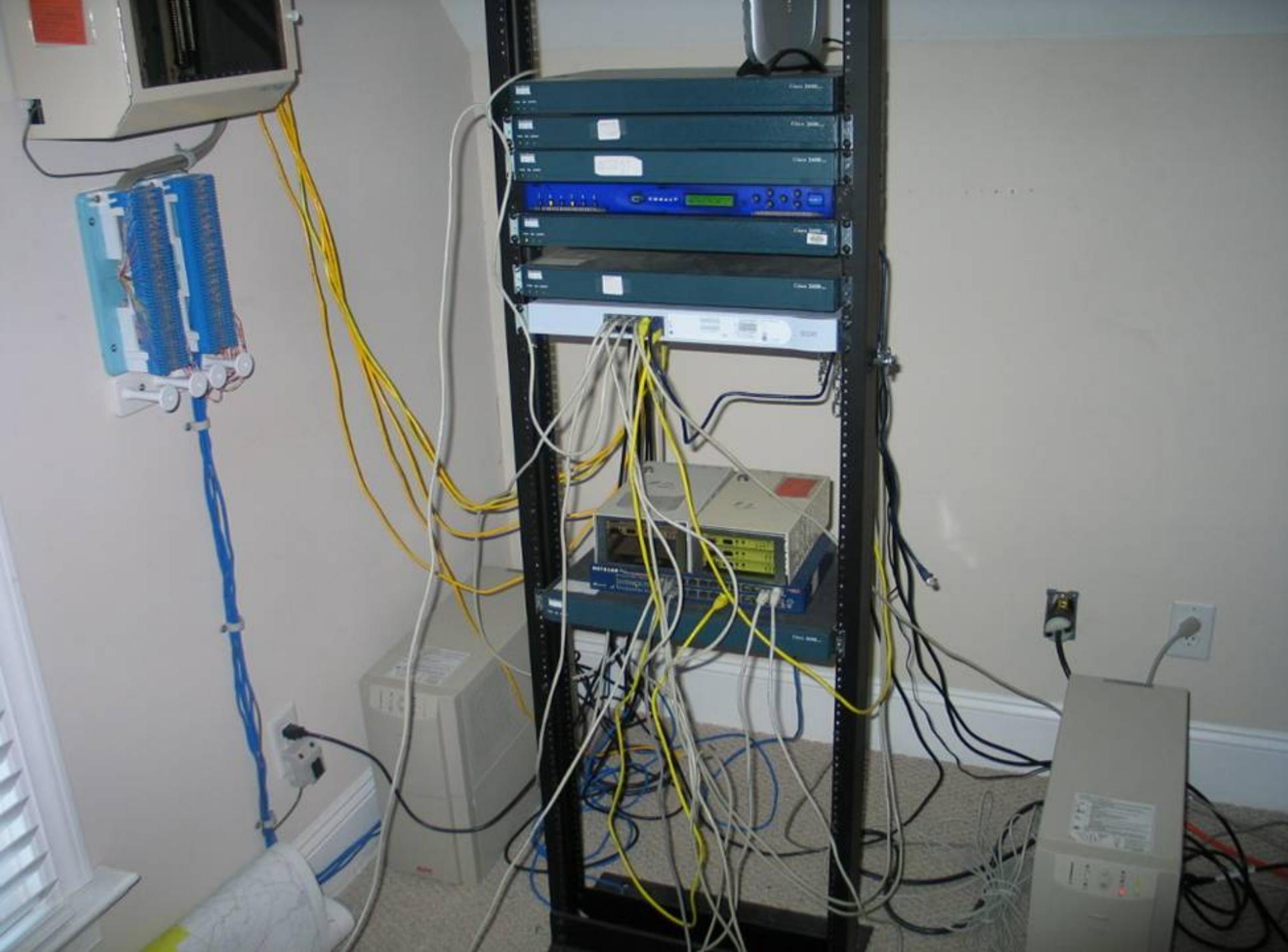
Virginia Attorney General's Office











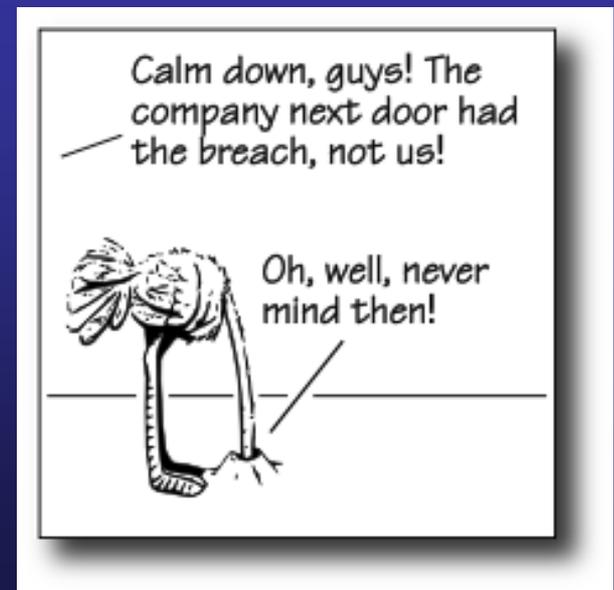
Outline

- Database Breaches
- Identity Theft
- VA Computer Crimes Act

Database Breaches

There are two types of companies in the world: those that know they've been hacked, and those that don't.

Misha Glenny





2015 DATA BREACH INVESTIGATIONS REPORT

\$400 MILLION

The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

2015 DBIR Contributors

(See Appendix C for a detailed list.)

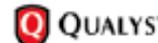
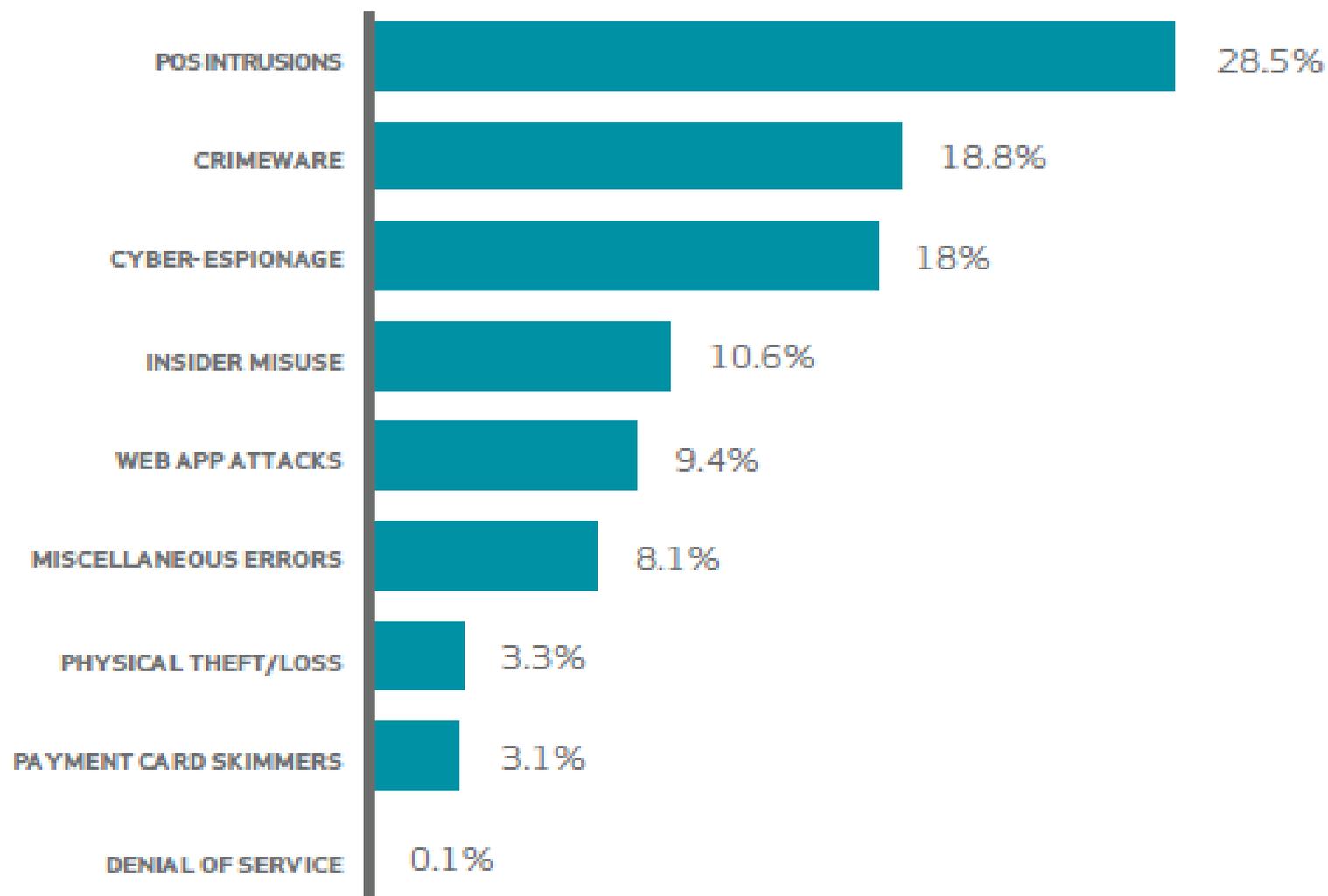


Figure 25.

Frequency of incident classification patterns with confirmed data breaches (n=1,598)

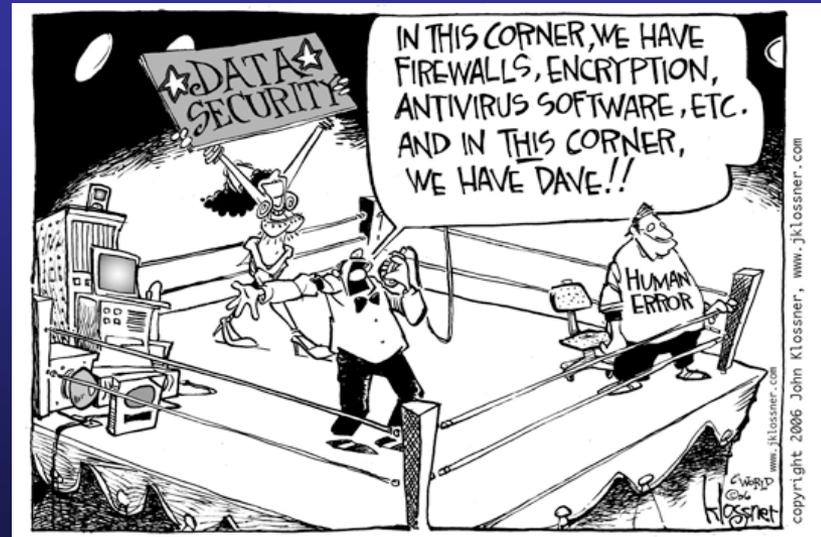


High-Profile Database Breaches

- Target --- 40M credit cards
- Home Depot --- 56M credit cards
- JP Morgan --- 83M email/physical addresses
- Anthem --- 80M records, including SSNs
- IRS --- 104,000 taxpayers
- OPM --- 4M employees' records

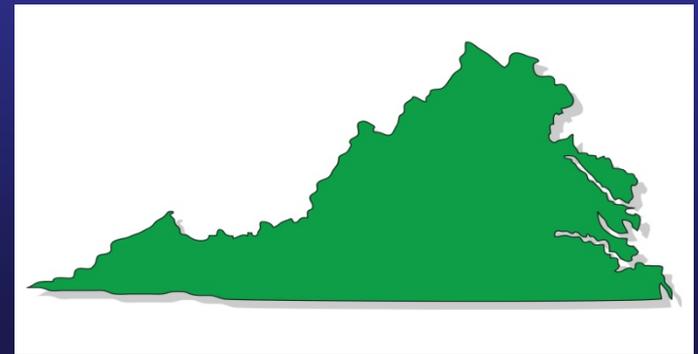
What are we seeing?

- 305 database breach notices received in Virginia in 2014
- Broad cross-section of industry
- Lost equipment, theft, intrusion are most common occurrences
- Small breaches dominate



Enforcer's Perspective

- From 1 resident to over 1 million residents affected in a single breach
- Work with your attorneys
- Contact law enforcement
- Work with our office



Database Breach Laws

- 47 states have data breach law
- Virginia Code Section 18.2-186.6
 - Took effect July 1, 2008
 - Crafted from Governor's consortium of national business and consumer advocates
 - Provides that compliance with Gramm-Leach-Bliley is sufficient

Virginia Data Breach Law

- Applies to any legal entity; broad application
- “Breach” defined as access to unencrypted, unredacted data by unauthorized person
- Must have caused or *reasonably believe* will cause fraud or identity theft to Virginia resident
- Must notify OAG and affected resident without *unreasonable delay*

Virginia Data Breach Law

- “Unreasonable delay” is undefined
 - Notice may be delayed to allow for determination of scope and to restore system integrity
 - Notice may be delayed at law-enforcement agency’s request
- Provisions also apply to encrypted data acquired in an unencrypted form or if person has access to the encryption key

Virginia Data Breach Law

- Data = “personal information”
 - First name or first initial and last name
 - Combined with one of the following
 - Social Security number
 - Driver’s license number
 - Financial account or credit card number in combination with security code, access code, or password
- Does not include publicly available information

Virginia Data Breach Law

- Notice = written, electronic, telephone or substitute
- Substitute Notice = over \$50K in cost, over 100,000 residents, or no sufficient contact info...can then post conspicuously on website or notify statewide media
- If more than 1,000 affected residents, must also notify consumer reporting agencies

Virginia Data Breach Law

- Notice must include:
 - Incident in general terms
 - Type of information accessed
 - Telephone number for affected persons to call
 - Advice directing person to remain vigilant of accounts and monitor free credit reports
 - The general acts of entity to prevent further unauthorized access



NEED DUCT TAPE
FROM AISLE 6 !!
PLUMBER'S PUTTY
FROM AISLE 5 !!
MOPS FROM
AISLE 2 !!

DATA
BREACH

THE
HOME
DEPOT

Virginia Data Breach Law

- Attorney General's Office can bring civil enforcement action for failure to comply with notice provisions
 - \$150,000 penalty per breach
 - Does not prohibit affected residents from filing individual claims



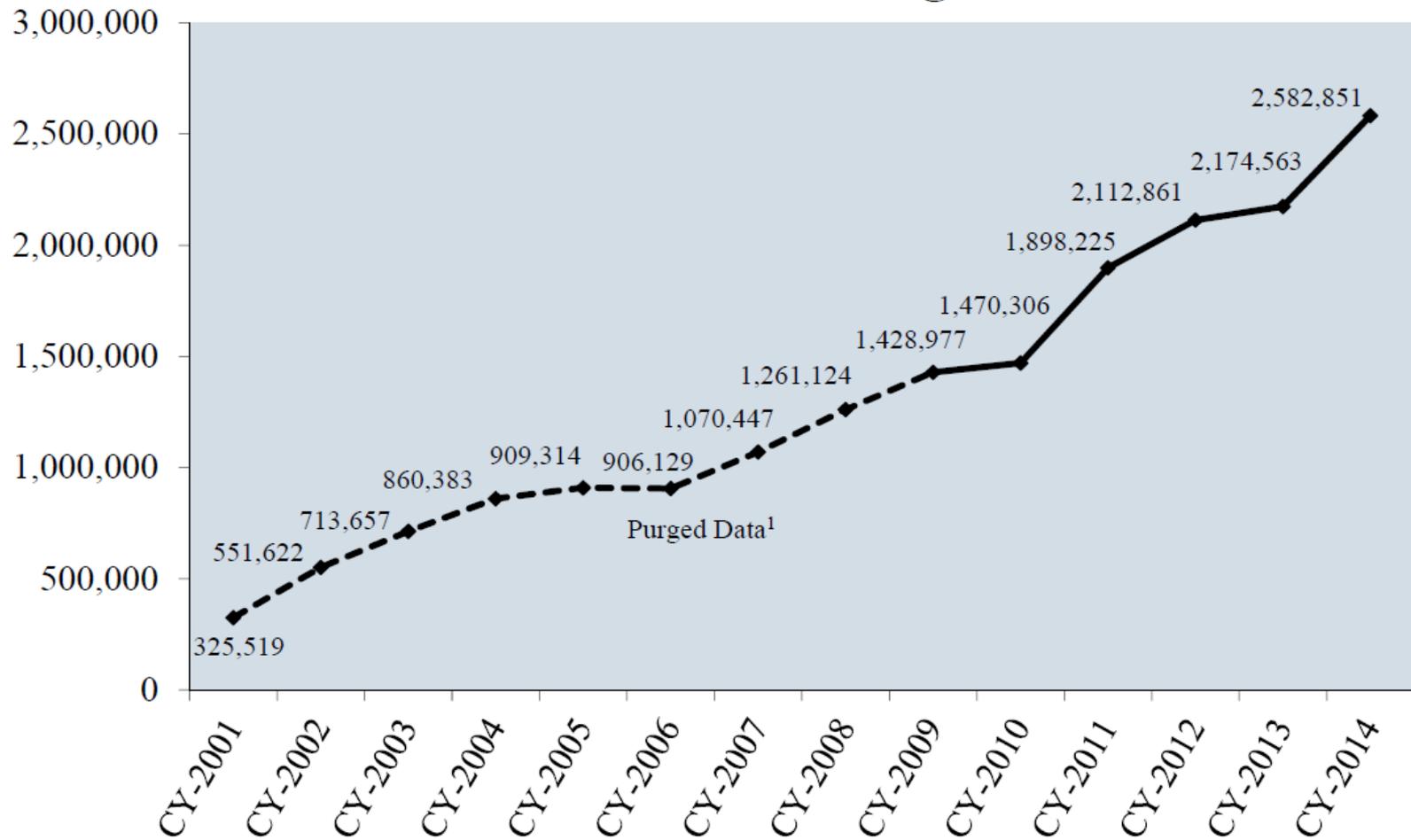
CONSUMER
SENTINEL NETWORK
DATA BOOK
for January – December 2014





Consumer Sentinel Network Complaint Count¹

Calendar Years 2001 through 2014



Consumer Sentinel Network State Complaint Rates

January 1 – December 31, 2014

Fraud & Other Complaints

Rank	Consumer State	Population ¹	Complaints Per 100,000
1	Florida	1,007.3	200,392
2	Georgia	777.7	78,526
3	Nevada	773.2	21,952
4	Delaware	769.2	7,197
5	Michigan	749.2	74,244
6	Maryland	675.5	40,369
7	Texas	647.2	174,468
8	California	644.6	250,138
9	New Jersey	598.9	53,535
10	Colorado	598.6	32,060
11	Virginia	594.9	49,537
12	Rhode Island	589.4	6,219
13	Alabama	574.2	27,847
14	Tennessee	570.2	37,347
15	New Hampshire	562.6	7,464
16	Arizona	562.1	37,836
17	Massachusetts	554.8	37,422
18	Pennsylvania	544.7	69,655
19	Louisiana	538.9	25,059
20	South Carolina	534.2	25,816
21	Missouri	516.3	31,304
22	New York	514.0	101,497
23	Washington	511.6	36,127
24	Connecticut	509.1	18,312
25	Wyoming	508.1	2,968
26	North Carolina	507.9	50,504
27	Ohio	506.3	58,704
28	New Mexico	506.1	10,556
29	Oregon	505.5	20,069
30	Illinois	473.9	61,038
31	West Virginia	466.6	8,634
32	Arkansas	465.2	13,800



Identity Theft Complaints

Rank	Victim State	Population ¹	Complaints Per 100,000
1	Florida	186.3	37,059
2	Washington	154.8	10,930
3	Oregon	124.6	4,946
4	Missouri	118.7	7,195
5	Georgia	112.7	11,384
6	Michigan	104.3	10,338
7	California	100.5	38,982
8	Nevada	100.2	2,846
9	Arizona	96.0	6,460
10	Maryland	95.9	5,734
10	Texas	95.9	25,843
12	Illinois	95.6	12,317
13	Colorado	85.5	4,579
14	Connecticut	85.4	3,071
15	Arkansas	83.6	2,481
16	Pennsylvania	81.7	10,446
17	New York	80.8	15,959
18	Mississippi	80.5	2,409
19	New Jersey	79.9	7,144
20	Ohio	79.0	9,161
21	Delaware	78.1	731
22	Alabama	77.7	3,770
23	New Mexico	77.2	1,611
24	Tennessee	76.2	4,993
25	Massachusetts	75.8	5,116
26	Wisconsin	74.4	4,283
27	Louisiana	73.8	3,430
27	North Carolina	73.8	7,334
29	Alaska	73.6	542
30	South Carolina	73.3	3,540
31	Virginia	71.1	5,921
32	Oklahoma	68.5	2,656



Fraud and Other Complaints Count from Virginia Consumers = 49,537

Top 10 Fraud and Other Complaint Categories Reported by Virginia Consumers

Rank	Top Categories	Complaints	Percentage ¹
1	Impostor Scams	6,268	13%
2	Debt Collection	5,594	11%
3	Banks and Lenders	3,778	8%
4	Telephone and Mobile Services	2,694	5%
5	Auto-Related Complaints	2,155	4%
6	Prizes, Sweepstakes and Lotteries	1,811	4%
7	Shop-at-Home and Catalog Sales	1,603	3%
8	Credit Bureaus, Information Furnishers and Report Users	1,370	3%
9	Television and Electronic Media	1,321	3%
10	Internet Services	1,193	2%

¹Percentages are based on the total number of CSN fraud and other complaints from Virginia consumers (49,537).

Identity Theft Complaints Count from Virginia Victims = 5,921

Identity Theft Types Reported by Virginia Victims

Rank	Identity Theft Type	Complaints	Percentage ¹
1	Government Documents or Benefits Fraud	2,069	35%
2	Credit Card Fraud	998	17%
3	Phone or Utilities Fraud	968	16%
4	Bank Fraud	560	9%
5	Loan Fraud	198	3%
6	Employment-Related Fraud	145	2%
	Other	1,263	21%
	Attempted Identity Theft	284	5%

¹Percentages are based on the 5,921 victims reporting from Virginia. Note that CSN identity theft complaints may be coded under multiple theft types.

Identity Theft

A. Unlawful for any person, without authorization . . . to:

1. Obtain, record or access identifying information which is not available to the general public that would assist in accessing financial resources...;
2. Obtain money, credit, loans, goods or services through the use of identifying information of such other person;
3. Obtain identification documents in such other person's name

Identity Theft

A. Identifying Information

- (i) name;
- (ii) date of birth;
- (iii) social security number;
- (iv) driver's license number;
- (v) bank account numbers;
- (vi) credit or debit card numbers;
- (vii) personal identification numbers (PIN);
- (viii) electronic identification codes;
- (ix) automated or electronic signatures;
- (x) biometric data;
- (xi) fingerprints;
- (xii) passwords; or
- (xiii) any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain money, credit, loans, goods, or services.

Identity Theft

- Penalties

- Up to 12 months jail
- If over \$200, 1-5 years imprisonment
- If 50 or more person's identifying info stolen, 1-5 years
- 1-10 years if information is used to commit another crime

Identity Theft

WHAT CAN YOU DO?

- Protect your social security number
- Use caution when giving out personal info
- Treat your trash carefully
- Protect your postal mail
- Check your bank statements often
- Use common sense

Identity Theft

WHAT CAN YOU DO?

- Check your credit reports (one free report annually)
 - Annualcreditreport.com (recommended by FTC)
- Protect your computer (firewall, anti-virus, lock wireless networks)
- Keep software updated

Identity Theft

- WHAT CAN YOU DO?
 - Create strong, distinct passwords
 - Do not base passwords on personal information that can be easily accessed or guessed
 - Do not use words that can be found in a dictionary
 - Use different passwords on different systems
 - Sign up for password-protection service, such as LastPass
 - Take advantage of two-step verification

Identity Theft

HOW TO SPOT IT...

- You see withdrawals from your bank account that you can't explain
- You don't get your bills or other mail
- Debt collectors call you about debts that aren't yours
- You find unfamiliar accounts or charges on your credit report

Identity Theft

WHERE TO REPORT IT...

- Creditors (Card Issuers & Utilities)
- Credit Bureaus
- Federal Trade Commission (FTC)
- Local/State Law Enforcement
- Office of the Attorney General

Protection of PII by State Agencies

– Section 2.2-3800

- Ensures safeguards for personal privacy by state and local agencies
- Need for PII must be clearly established and policies put in place to prevent misuse

– Section 42.1-82

- Prescribes procedures for disposal, physical destruction of public records with SSNs by:
 - Shredding
 - Deleting
 - Redacting SSN to make unreadable or undecipherable

VA Computer Crimes

- Virginia Computer Crimes Act
 - Computer Fraud
 - SPAM
 - Computer Trespass
 - Computer Invasion of Privacy
 - Theft of Computer Services
 - Harassment by Computer
 - Using Computer to Gather ID Info (Phishing)
 - Civil Provision

VA Computer Crimes

- Computer Trespass

- Unlawful, with malicious intent, to:
 - Remove, halt, or disable computer data or program
 - Cause a network to malfunction
 - Alter, disable, or erase computer data, programs, or software
 - Effect the creation or alteration of financial instruments
 - Use a computer to cause physical injury to property
 - Use a computer to make unauthorized copy
 - Install keystroke logger
 - Install software to take control of computer in order to cause damage or disrupt transmissions

VA Computer Crimes

- Computer Trespass, cont.
 - Penalties:
 - Up to 12 months jail
 - Damage over \$1K, 1-5 years imprisonment
 - Installs software on more than 5 computers, 1-5 years
 - Keystroke logger violation, 1-5 years
 - Exception for ISPs

VA Computer Crimes

- Computer Fraud

- Use a computer without authority to:
 - Obtain property or services by false pretenses
 - Embezzle or commit larceny
 - Convert the property of another
- Value is \$200 or more – 1-10 years imprisonment
- Otherwise up to 12 months in jail

VA Computer Crimes

- Phishing

- Using a computer to gather identifying information
- A. Unlawful to use a computer to obtain, access, or record, through the use of material artifice, trickery or deception, any identifying information – 1-5 years imprisonment
- B. Distribution of material – 1-10 years
- C. Uses such information to commit another crime – 1-10 years

Phishing Variations

- Banking Trojans
 - Website-based
- “Vishing”
 - VOIP-based
 - Threaten legal action without payment
- Spear Phishing
 - Internet- or email-based email targetting specific individual

VA Computer Crimes

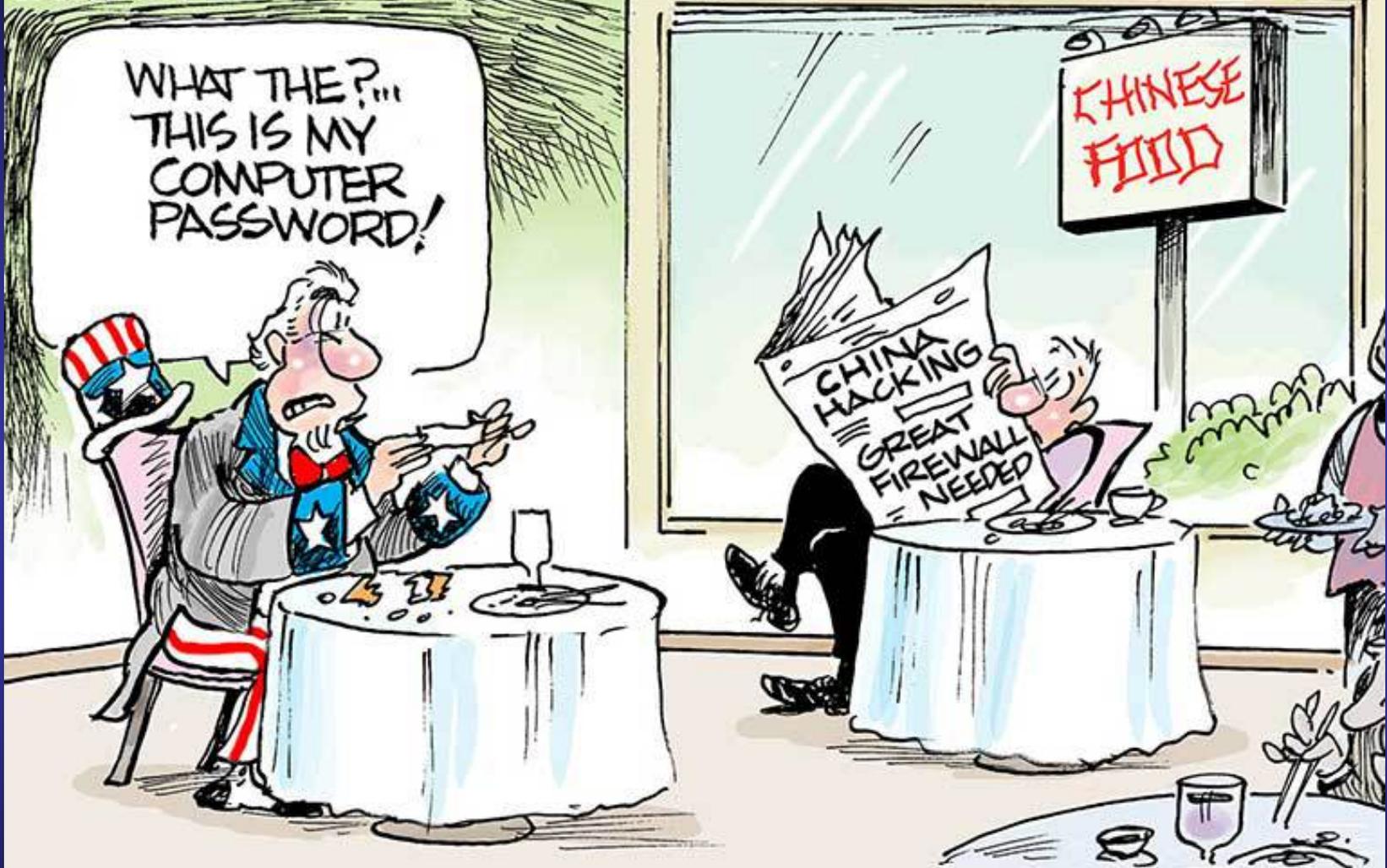
- Civil Remedy

- Any individual wronged by any violation of aforementioned prohibitions may bring suit
- For any damages sustained and cost of suit
- Loss of profits
- Malicious intent NOT required

WHAT THE?...
THIS IS MY
COMPUTER
PASSWORD!

CHINESE
FOOD

CHINA
HACKING
GREAT
FIREWALL
NEEDED



RESOURCES

VA Office of the Attorney General

<http://www.ag.virginia.gov>

Internet Crime Complaint Center

<http://www.ic3.gov>

Federal Trade Commission (FTC)

<http://www.ftc.gov>

Thank You

Tommy Johnstone

Assistant Attorney General

Virginia Attorney General's Office

tjohnstone@oag.state.va.us

804-786-2071

www.ag.virginia.gov



Virginia Information Technologies Agency

Upcoming Events





IS Orientation

When: Thursday, September 24, 2015

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1211

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



Future ISOAG

August 5, 1:00 - 4:00 pm @ CESC

Speaker: Ben Sady of Dixon Hughes Goodman

ISOAG meets the 1st Wednesday of each month in 2015



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov

ADJOURN

THANK YOU FOR ATTENDING

