

MARYLAND COMMISSION ON CONSUMER FINANCIAL PROTECTION

Wednesday, September 12, 2018

MD|DC Credit Union Association



MD|DC
Credit Union Association

Engage · Influence · Impact

DATA BREACHES

DATA RECORDS COMPROMISED IN 2017

2,600,968,280

7,125,940

records lost or stolen
every day



296,914

records
every hour



4,949

records
every minute



82

records
every second



LESS THAN **4%** of breaches were “**Secure Breaches**” where **encryption** rendered the stolen data useless

Source: Gemalto

DATA BREACH BY INDUSTRY

Records Stolen/Lost By Industry

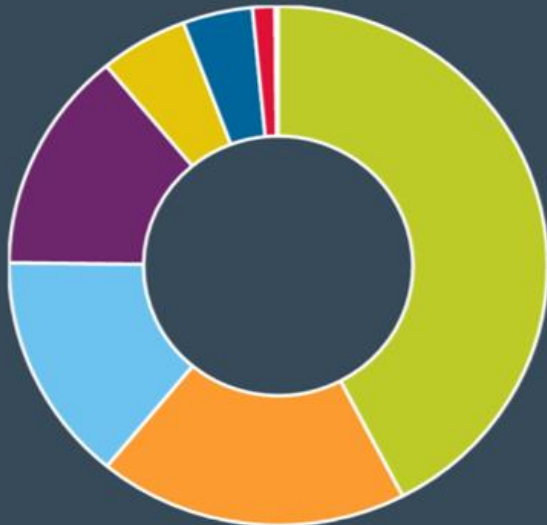
Breach Incidents By Source

Breach Incidents By Type

DATA RECORDS STOLEN OR LOST BY INDUSTRY

Shows percentage of total records, hover over pie chart for record totals.

Date Range: 2013 - Present



Technology

35.19%

Other

15.46%

Retail

11.82%

Government

11.46%

Financial

4.40%

Healthcare

3.48%

Education

1.12%

DATA BREACH DEFINED

What is a
data breach?

An incident in which an individual name plus a social security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure.



TYPES OF DATA BREACHED

- Social Security Number
- Credit/Debit Card Number
- Email/Password/Username
- Protected Health Information
- Individual Taxpayer ID Number
- Driver's License
- Financial Accounts
- Publicly Identifiable Information



DATA BREACH TACTICS



Insider Theft



Hacking (Phishing, Ransomware/Malware, Skimming)



Data on the Move



Physical Theft



**Employee Error / Negligence /
Improper Disposal / Lost**

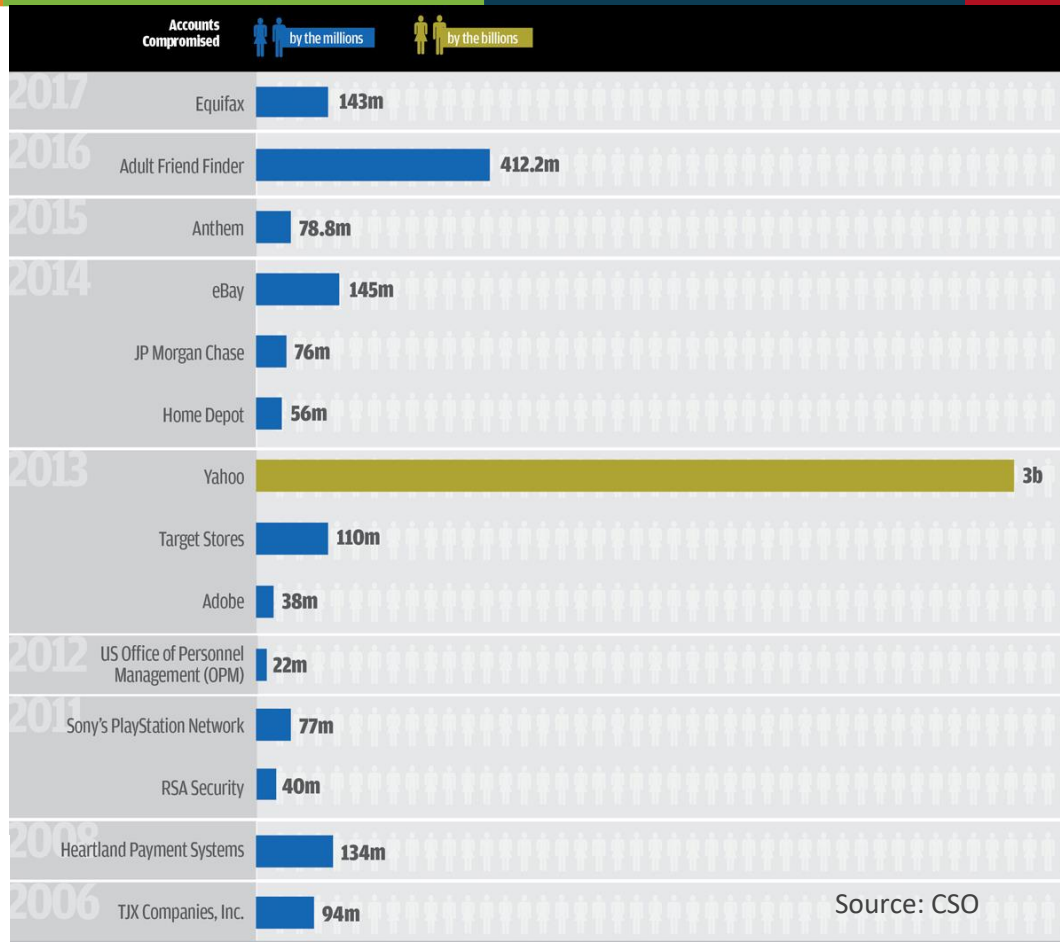


Accidental Web/Internet Exposure



Unauthorized Access

DATA BREACHES: IMPACT



OPM DATA BREACH: 2012

Data of 21.5 Million people compromised

- **Social security numbers**
- **Residency & education history**
- **Employment history**
- **Information on family, criminal and financial history**

May also have included:

- **Interview notes taken by background investigators**
- **Fingerprints**

FRAUD TRENDS



SYNTHETIC FRAUD

- Use piecemeal data to create a new, fictitious identity
- Children and elderly most often targets

FRAUD TRENDS



CARD NOT PRESENT

- Telephone, Internet and mail order transactions
- Data obtained through skimming, hacking, email phishing or telephone solicitations

FRAUD TRENDS



ACH FRAUD

- Automated Clearing House Network exploited
- Account and routing numbers stolen
- Information used to transfer funds or make payments

FRAUD TRENDS



WIRE TRANSFER FRAUD

- Relative in Need
- Sweepstakes
- Debt Collection
- Online Dating
- Employment Related

FRAUD TRENDS

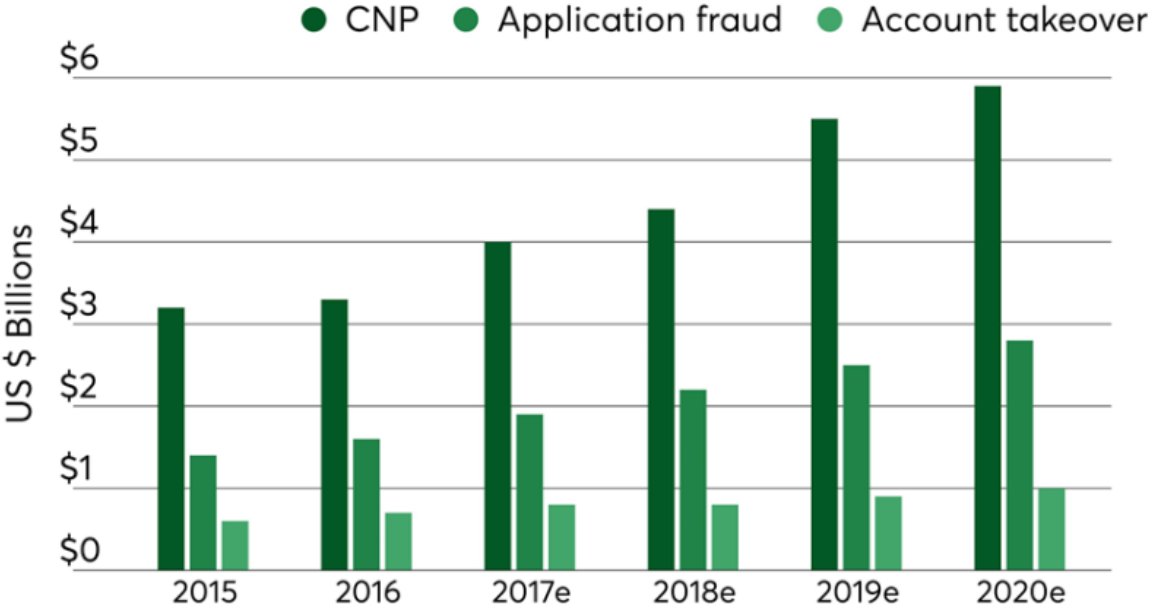


CARD SKIMMING

- Card reading devices placed inside payment terminals
- Extracts information from card
- Make fraudulent charges and counterfeit cards

FRAUD TRENDS

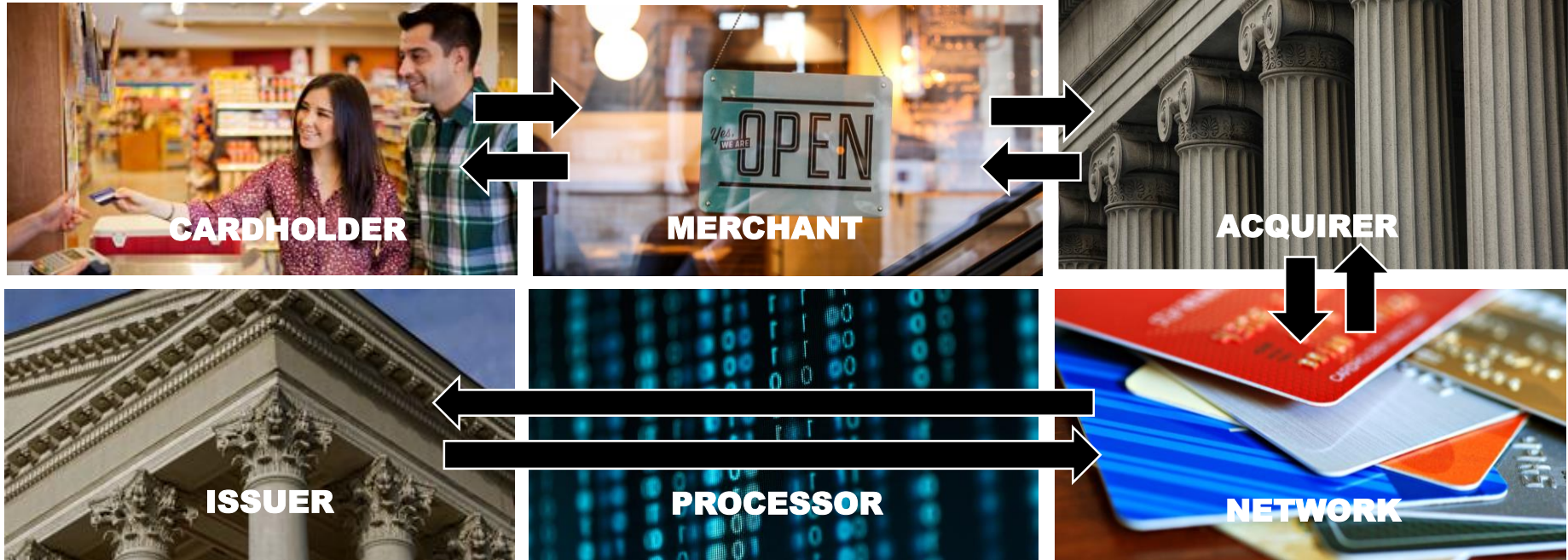
CNP fraud growing in the U.S.



Source: Aite



CREDIT CARD TRANSACTION FLOW



THE PAYMENTS ECOSYSTEM 2017

ACQUIRERS/ PROCESSORS



CARD NETWORKS



ISSUERS



GATEWAYS

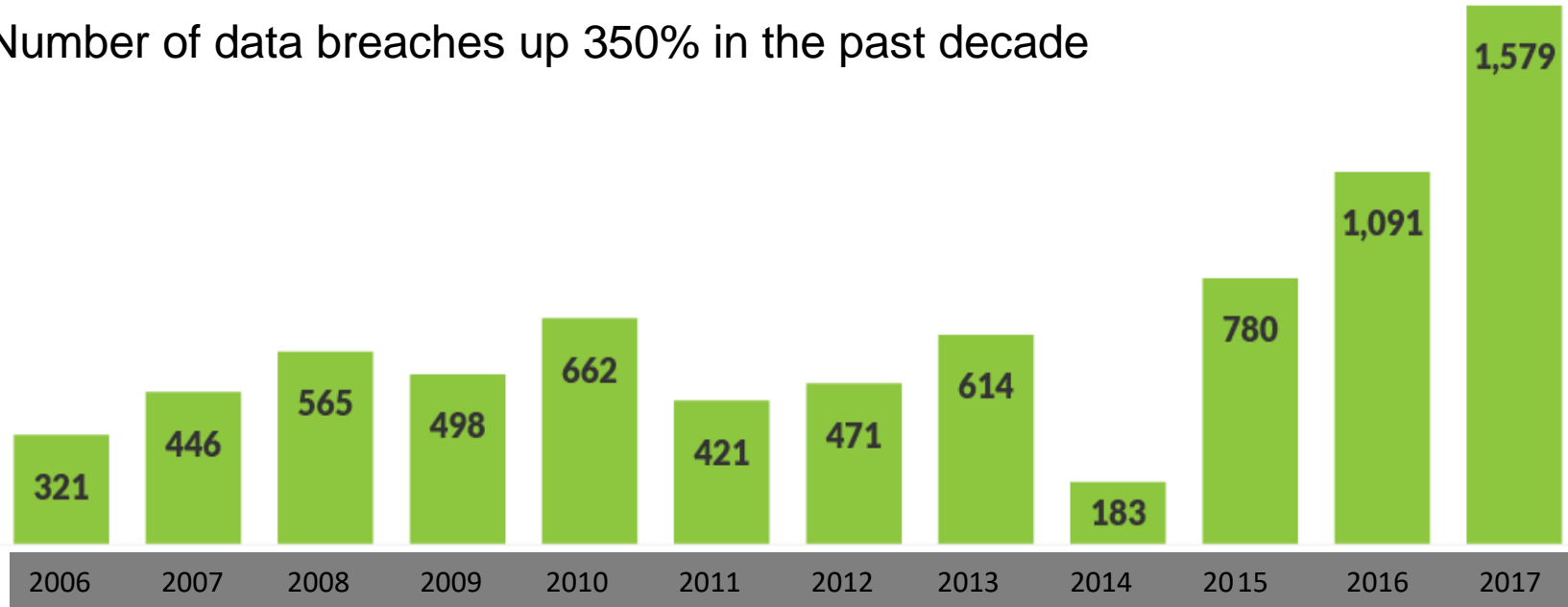


ISOs / MSPs



CURRENT STATE OF FRAUD

Number of data breaches up 350% in the past decade





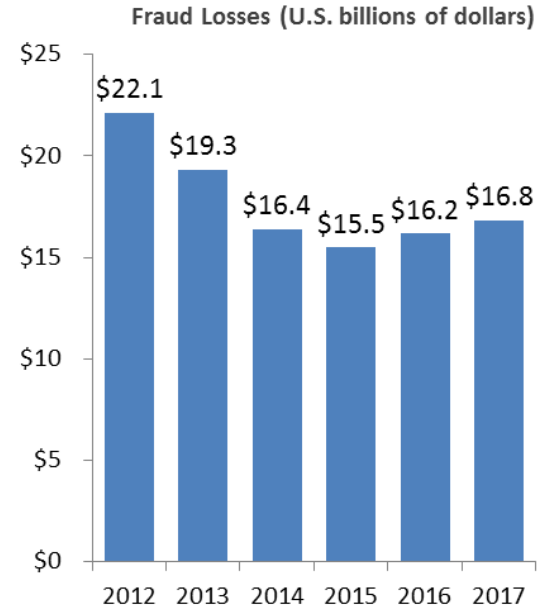
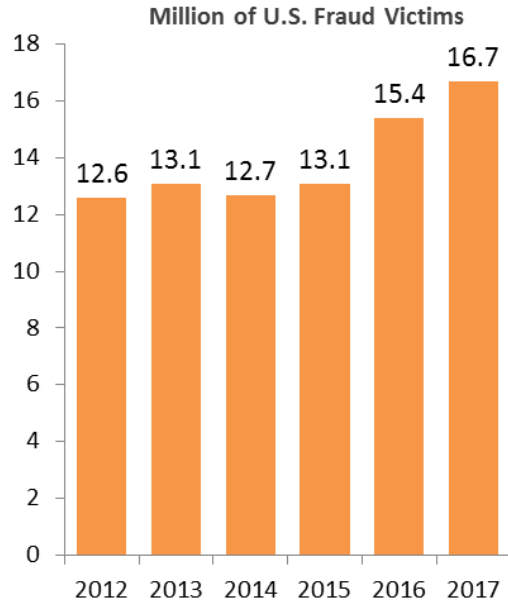
1.7 Billion
Reported data
breaches in
first half of 2018



15.4 Million
ID theft victims
in 2017, up 27%
from 2015

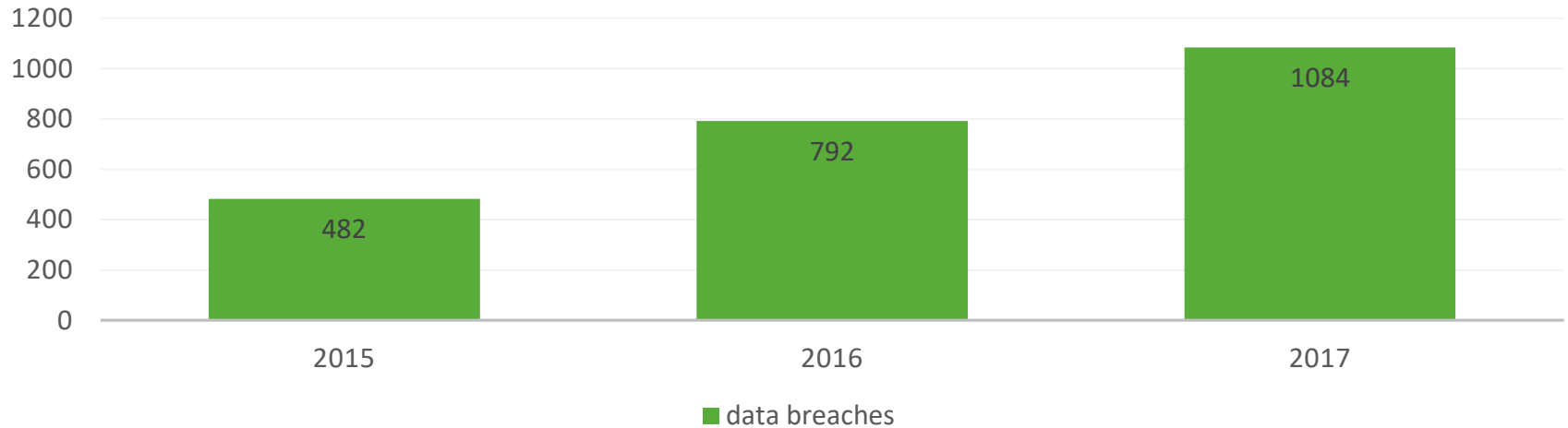
FRAUD VICTIMS & LOSSES NATIONWIDE

Fraud Victims and Losses Continue Three-Year Rise



DATA BREACHES IN MARYLAND

548 data breaches through June 2018



Source: Maryland Office of the Attorney General

2017 STATE RANKINGS: IDENTITY THEFT REPORTS

RANK	STATE	REPORTS PER 100K POPULATION	NUMBER OF REPORTS
1	Michigan	151	15,027
2	Florida	149	31,167
3	California	140	55,418
4	Maryland	129	7,787
5	Nevada	128	3,828

Source: Federal Trade Commission
Consumer Sentinel Network Data Book 2017

FRAUD IMPACT ON CONSUMER BEHAVIOR

INFOGRAPHIC

How Fraud Affects Consumer Card Use

According to a new survey released by Sparks Research and fraud prevention firm Tender Armor, fraud has caused most online shoppers to use their debit and credit cards less. Here's a look at the key findings of the survey, which questioned 1,013 e-commerce credit and debit card shoppers in Q1 2016.

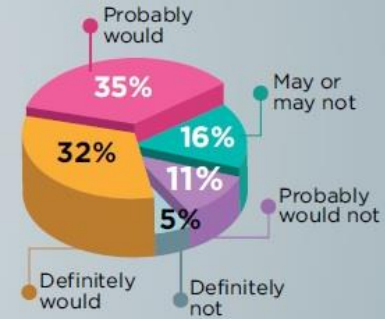
Which statement best matches your final thoughts about online shopping after a fraudulent charge?



Which statement best sums up your feelings toward online purchases?



Would you use a card feature that replaced the security code printed on your payment card with a daily code?



MD FRAUD LOSSES

Total Fraud Losses
\$12.4 Million

Median Fraud Loss
\$458

Source: Federal Trade Commission
Consumer Sentinel Network Data Book 2017

STATE DATA BREACH LAWS

Holding Out

Four states have yet to enact a data breach notification law:
Alabama, Kentucky, New Mexico and South Dakota.

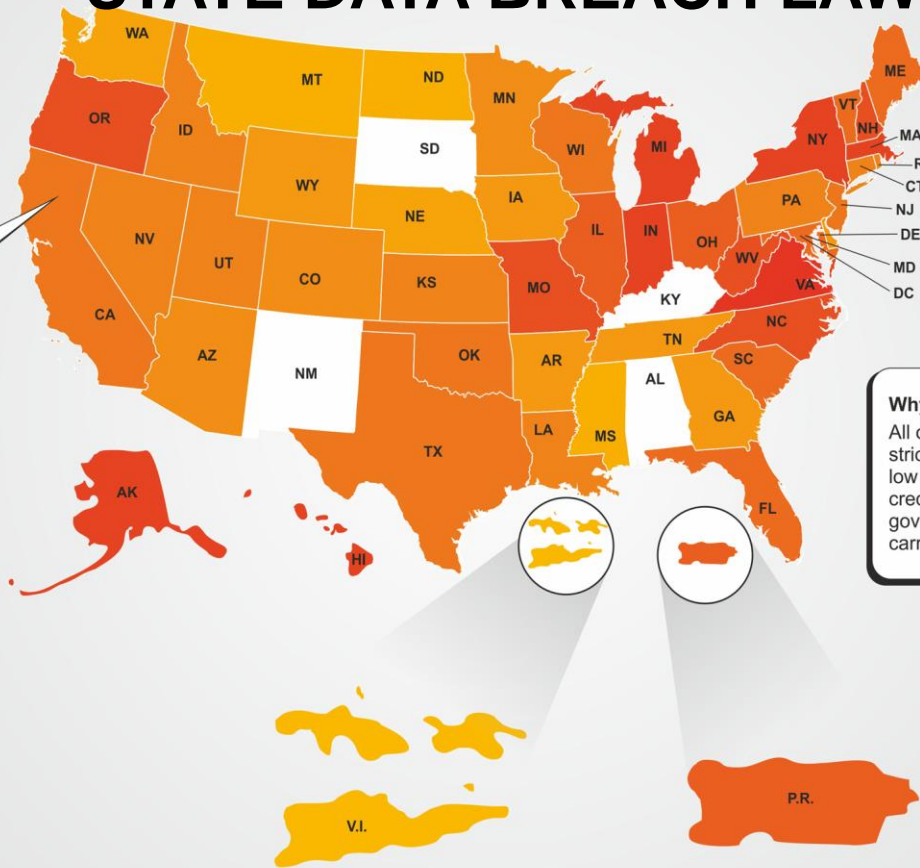
The Original Standard

California was the first state to enact data breach notification legislation. The law went into effect on July 1, 2003. Outside the scope used in this analysis, California's laws include provisions specifically for credit reporting agencies and for businesses owning or maintaining medical data. Other states carry these provisions as well.

Why Certain States Stand Out

All of the laws are strict, but the stricter laws include a relatively low bar triggering notification to credit reporting agencies and government entities. They also carry higher maximum fines.

*Note: A score of zero means a data breach notification law does not exist in that state.



State	Score
AL	0
KY	0
NM	0
SD	0
V.I.	5
ND	6
MS	7
MT	7
NE	7
WA	7
AR	8
DE	8
GA	8
IA	8
TN	8
WY	8
AZ	9
CO	9
MN	9
CT	10
ID	10
KS	10
LA	10
NV	10
PA	10
RI	10
UT	10
CA	11
NJ	11
OK	11
TX	11
WI	11
DC	12
FL	12
MD	12
ME	12
SC	12
VT	12
IL	13
OH	13
P.R.	13
MO	14
NC	14
NH	14
OR	14
WV	14
AK	15

Less strict



More strict

Key: The darker the state, the more strict the law

BEYOND NOTIFICATION LAWS

State	Examples of Violation Penalties (not intended to reflect full statute)
Maryland	Violations constitute an unfair or deceptive trade practice under Title 13 of the Maryland Code
Alabama	Entities could be liable for civil penalties up to \$5,000 per day for each consecutive day the entity fails to take reasonable action to comply with notice provisions, with the total civil penalty not to exceed \$500,000.
Florida	Failure to provide notice within 30 days: \$1,000 per day for first 30 days following violation , then up to \$50,000 for each subsequent 30-day period up to 180 days, not to exceed \$500,000 if violation continues. Penalties apply per breach, not per affected individual.
Minnesota	A civil penalty, in an amount to be determined by the court, not in excess of \$25,000 .
Missouri	For willful and knowing violations, actual damages and/or civil penalties not to exceed \$150,000 for each breach .
N.H.	Civil penalties up to \$10,000 per violation .
New York	Knowing or willful violations, civil penalties of the greater of \$5,000 or up to \$10,000 per instance of failed notification, provided that the latter amount may not exceed \$150,000.
Texas	Civil penalty of at least \$2,000 but not more than \$50,000 for each violation . Failure to take reasonable corrective action to comply with the statute can result in additional penalties of \$100 per individual per day of failed or delayed notification, not to exceed \$250,000 for a single breach .
Virginia	A.G. may bring an action and may impose a civil penalty not to exceed \$150,000 per security breach or a series of breaches of a similar nature that are discovered in a single investigation.

FEDERAL LEGISLATION

- **H.R. 6743** introduced Sept. 7 by Rep. Luetkemyer - House Financial Services Committee
- Applies only to financial services sector
- Creates regulatory framework requiring timely notice to impacted consumers, law enforcement & regulators
- Preemption of state laws



MOVING FORWARD

- All members of the marketplace need to be subject to the same stringent data security standards
- The cost of data breaches should be borne by the entity responsible for the breach
- Any solution should be comprehensive, not narrowly focused

THANK YOU

CONTACTS:

- John Bratsakis
MD|DC Credit Union Association
President/CEO
jbratsakis@mddccua.org | 443.325.0774
- Rory Murray
MD|DC Credit Union Association
Director, Legislative Affairs
rmurray@mddccua.org | 443.325.0775