MARYLAND COMMISSION ON CONSUMER FINANCIAL PROTECTION

Wednesday, September 12, 2018

MD|DC Credit Union Association
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

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%
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

Source: CSO
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

- **Cardholder**
- **Merchant**
- **Acquirer**
- **Issuer**
- **Processor**
- **Network**
### THE PAYMENTS ECOSYSTEM 2017

<table>
<thead>
<tr>
<th>ACQUIRERS/PROCESSORS</th>
<th>Adyen</th>
<th>Barclays</th>
<th>Cielo</th>
<th>Elavon</th>
<th>Fiserv</th>
<th>Heartland</th>
<th>TSYS</th>
<th>Wells Fargo</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bank of America</td>
<td>CHASE Paymentech</td>
<td>Citi</td>
<td>First Data</td>
<td>Global Payments</td>
<td>Moneris Solutions</td>
<td>Vantiv</td>
<td>Worldpay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CARD NETWORKS</th>
<th>Accel</th>
<th>Discover</th>
<th>Interlink</th>
<th>Maestro</th>
<th>NYCE</th>
<th>Pulse</th>
<th>Star</th>
<th>Visa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>American Express</td>
<td>Interac</td>
<td>JCB</td>
<td>Mastercard</td>
<td>Plus</td>
<td>Shazam</td>
<td>UnionPay Emb</td>
<td>Visa ReadyLink</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISSUERS</th>
<th>American Express</th>
<th>Barclays</th>
<th>Capital One</th>
<th>Citi</th>
<th>HSBC</th>
<th>Illusion Pay</th>
<th>US Bank</th>
<th>Wells Fargo</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bank of America</td>
<td>Cabela's Club</td>
<td>CHASE</td>
<td>Discover</td>
<td>PNC</td>
<td>TD Bank</td>
<td>USAA</td>
<td>WCX</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GATEWAYS</th>
<th>2Checkout.com</th>
<th>Alipay</th>
<th>Beanstream</th>
<th>Braintree</th>
<th>Klarna</th>
<th>PaySafe</th>
<th>Square</th>
<th>WePay</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Adyen</td>
<td>Authorize.Net</td>
<td>Bluesnap</td>
<td>CardConnect</td>
<td>PayPal</td>
<td>Sage Pay</td>
<td>Stripe</td>
<td>Worldpay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISOs / MSPs</th>
<th>CreditCard Processing.com</th>
<th>Everlink</th>
<th>Flagship</th>
<th>Merchant One</th>
<th>North American Bancard</th>
<th>Paywire</th>
<th>Priority Payment Systems</th>
<th>Total Merchant Services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cayan</td>
<td>Evo</td>
<td>Merchant e-Solutions</td>
<td>National Bankcard</td>
<td>OpenEdge</td>
<td>Pivotal</td>
<td>The Transaction Group</td>
<td>Versapay</td>
</tr>
</tbody>
</table>
CURRENT STATE OF FRAUD

Number of data breaches up 350% in the past decade

Source: Identity Theft Resource Center
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 and Losses Continue Three-Year Rise

Source: 2018 Identity Fraud Study, Javelin Strategy & Research
DATA BREACHES IN MARYLAND

548 data breaches through June 2018

Source: Maryland Office of the Attorney General
<table>
<thead>
<tr>
<th>RANK</th>
<th>STATE</th>
<th>REPORTS PER 100K POPULATION</th>
<th>NUMBER OF REPORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Michigan</td>
<td>151</td>
<td>15,027</td>
</tr>
<tr>
<td>2</td>
<td>Florida</td>
<td>149</td>
<td>31,167</td>
</tr>
<tr>
<td>3</td>
<td>California</td>
<td>140</td>
<td>55,418</td>
</tr>
<tr>
<td>4</td>
<td>Maryland</td>
<td>129</td>
<td>7,787</td>
</tr>
<tr>
<td>5</td>
<td>Nevada</td>
<td>128</td>
<td>3,828</td>
</tr>
</tbody>
</table>

Source: Federal Trade Commission
Consumer Sentinel Network Data Book 2017
FRAUD IMPACT ON CONSUMER BEHAVIOR

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?

- Closed the account: 15%
- Changed online retailers: 14%
- Shopped less online: 12%
- Used replacement card less: 12%
- Did not use replacement card: 3%

Which statement best sums up your feelings toward online purchases?

- Would like more assurance that card is secure: 48%
- Enjoyed the convenience of one-click buy buttons: 20%
- Don’t think twice about financial security: 9%
- Afraid of getting identity stolen: 6%
- Don’t like the hassle: 6%

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

- Probably would: 35%
- May or may not: 16%
- Probably would not: 5%
- Definitely would: 32%
- Definitely not: 11%

78% of online shoppers want more protection for their payment card data when shopping online.

56% of consumers changed shopping behaviors after a fraud event.

67% of consumers are willing to adopt a new behavior to increase their security when shopping online.

Data source: Sparks Research Online Shopper Survey: 2016
Total Fraud Losses
$12.4 Million

Median Fraud Loss
$458

Source: Federal Trade Commission
Consumer Sentinel Network Data Book 2017
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.
## BEYOND NOTIFICATION LAWS

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

- **H.R. 6743** introduced Sept. 7 by Rep. Luetkeymeyer - 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
• 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