LegalShield
BUSINESS SOLUTIONS

A LegalShield Presentation

Identity Theft

Be Prepared..
Be Proactive!

Hosted by:

Barry J. Olfern & Carmen Bernard
Independent LegalShield Associates

417 Million Non-sensitive Records Exposed in February 2019

Identity theft has been one of the top consumer complaints filed with the FTC for **16 years straight.**

February Data Breaches by Industry **In February 2019 there were a total of 101 data breaches, which exposed 2,064,279 sensitive records and an additional 417 million (417,827,304) non-sensitive records.**

Of the total sensitive records exposed in February, 96 percent were exposed through the **Medical/Healthcare sector**.

Nearly 100 percent of the non-sensitive records exposed reported in February were attributed to only 18 of the 23 total breaches that reported both sensitive and non-sensitive records exposed in the **Business sector**.

INDUSTRY	# OF BREACHES	# OF SENSITIVE RECORDS EXPOSED	# OF NON-SENSITIVE RECORDS EXPOSED
Business	53	9,131	417,826,396
Medical/Healthcare	30	1,979,716	908
Government/Military	4	33,210	Unknown
Banking/Credit/Financial	7	Unknown	Unknown
Education	7	42,222	Unknown
MONTHLY TOTALS:	101	2,064,279	417,827,304

February Data Breaches by Method

- **Hacking** was the most common method of breach in February 2019 at 61 percent of the overall number of data breaches reported.
- **Unauthorized Access** was the second most common method of data breach at 20 percent of the overall number of data breaches for the month.
- **Hacking** was the key method responsible for nearly 100 percent of the non-sensitive records exposed that were reported in February 2019.

# OF DATA BREACHES PER METHOD PER INDUSTRY					
Method	Banking	Business	Education	Government	Medical
Insider Theft	0	1	0	0	0
Hacking/Intrusion (includes Phishing, Ransomware/Malware and Skimming)	5	37	3	1	16
Data on the Move	0	0	0	0	1
Physical Theft	0	2	0	0	2
Employee Error/Negligence/Improper Disposal/Lost	1	2	2	1	4
Accidental Web/Internet Exposure	0	0	1	1	1
Unauthorized Access	1	11	1	1	6

Year-over-Year Comparison

- Compared to February 2018 and February 2017, February 2019 had the least amount of data breaches reported yet had the **highest amount of sensitive records exposed**.

- Breaches of the **Medical/Healthcare sector** exposed the highest number of sensitive records in February 2019 and 2018, while breaches in **the Business sector exposed the highest amount of sensitive records in 2017.**

- **Hacking** was the **most common method** of breach in February for **all three years** representing 61 percent in 2019, 41 percent in 2018 and 71 percent in 2017 of the total number of breaches per year.

INDUSTRY	2019		2018		2017	
	# of breaches	sensitive records exposed	# of breaches	sensitive records exposed	# of breaches	sensitive records exposed
Business	53	9,131	62	221,380	139	780,750
Medical/Healthcare	30	1,979,716	26	937,354	30	147,144
Government/Military	4	33,210	17	405,404	10	41,749
Banking/Credit/Financial	7	0	23	29,714	11	88,008
Education	7	42,222	12	9,056	29	38,825

Identity Theft Facts

- Did you know someone falls victim to **identity theft every 2 seconds in America**? (Source: CNN)
- Did you know Americans are significantly more likely to be victims of identity theft than anyone else? **Over 791 million identities were stolen in the US in 2016.** (Source: Symantec)
- Did you know the average **time to solve a Medical Identity Theft is 12.1 months**? (Source: American Medical News Aug. 6, 2012)
- Did you know that **the personal cost of resolving Medical Identity Theft is $22,346 per victim?** (Source: American Medical News Aug. 6, 2012)
- Did you know that over **1 million children were Identity theft victims in 2017?** (Source: Javelin Strategy)
- 10% of identity-theft victims said **they experienced severe emotional distress as a result of the incident**. The level of victims' emotional distress was related to the time spent resolving problems. **More than a third (36%) of victims who spent 6 months or more resolving financial and credit problems as a result of the identity theft experienced severe emotional distress.** In comparison, 4% of victims who spent one day or less clearing up problems experienced severe distress. (Source: Bureau of Justice Statistics report "Victims of Identity theft, 2016) released January 2019

LegalShield® BUSINESS SOLUTIONS

Identity Theft Facts, cont.

- Identity theft is a crime that impacts the lives of more than **10 million consumers every year-and the numbers are increasing.**
- It's hard to imagine that **one out of every 20 consumers is at risk of being a victim this year alone.**
- The cost of identity theft among **consumers costs businesses worldwide an estimated $221 billion a year**, according to the Aberdeen Group.

However, consumers are no longer the only ones being targeted by these criminals. **Now business owners have a new kind of threat to be concerned about that can cause a whirlwind of devastation to a victim's business.**

Business identity theft is the newest threat to small businesses all across America. In the case of a business, **a criminal will seize a company's identity and use it to acquire credit in the company's name.**

Once they successfully obtain these credit accounts, the criminals will go on a spending spree buying electronics, office equipment, gift cards, and any other items that can be purchased and sold for cash.

The damage inflicted can cripple a business, prevent it from acquiring any credit, and even threaten its very operation while a victim is trying to clean up and recover from it.

LegalShield® BUSINESS SOLUTIONS

How to Prevent and Detect Business Identity Theft

The following five strategies can help you prevent and detect business identify theft:

1. Develop a protection plan – While most businesses focus on developing business plans to grow their company, little attention is paid to developing a protection plan. Design a step-by-step plan to protect your company's identity at the same time putting in place an action plan in the event that you do become a victim.

2. Protect company documents – Keep all your company documents and records in a safe and secure location. Dispose of any unnecessary information by using a micro cut shredder for the highest level of security. Also, never provide your company's federal tax identification number, financials, or bank statements to anyone unless you have made the initial contact. Finally, consider using a prepaid business credit card for employees as opposed to a traditional business credit card. With these cards you can set limits, deactivate a card in real time, and even limit the merchants for which the card can be used. If a criminal happens to steal a company card from an employee, you can quickly take action.

LegalShield® BUSINESS SOLUTIONS

How to Prevent and Detect Business Identity Theft, cont.

3. Protect company information online – One of the surefire ways to put your company at risk is by using sensitive information such as an employer identification number (EIN), account numbers, financial documents, or personal information via email or the web. If you must provide this information for a specific reason such as applying for credit, make sure the site is secure and its security certificate is up to date.

4. Monitor business credit reports – One of the fastest ways to detect a possible identity theft is to monitor your company's profiles with all three major business credit bureaus. You can accomplish this by subscribing to their monitoring services which give you access to your files 24/7. Take advantage of email alert notifications so you can be notified of any new activity occurring on your company credit files in real time.

5. Avoid the "master" user – You should avoid creating any type of "master" user account and password where an employee or individual can gain access to all your company information.

LegalShield®
BUSINESS SOLUTIONS

List of Large Breaches that you might have been exposed to even if you don't use the products.

- Adobe Systems October 2013: Products included: ColdFusion, Photoshop and Acrobat- **38 Million Accounts were affected, along with 3 million credit cards**.
- Special K Data Feed Spam List: October 2015: Email addresses
- KnownCircle Breach: Spam List- **1 Million people**: personal information: Criminals use spam lists to target and trick people online.
- Email Data List Breach- September 2017: **Over 192 Million unique email addresses** were collected and shared publicly.: Target you by email phishing or spamming campaign. Don't click on links or open attachments if you can't confirm where they're from.
- Collection #2 Combo List Breach: This is one of a series of 5 Collections of combo list: **3 Billion unique records**, including millions of exposed emails and passwords.
- 2019 Antipublic Combo List: **1.7 Billion**: Criminals use passwords from combolist to try and gain access to your other accounts.

LegalShield® BUSINESS SOLUTIONS

Prevent Identity Theft

Keep these tips in mind to protect yourself from identity theft

- **Secure your Social Security number** (SSN). Don't carry your Social Security card in your wallet. Only give out your SSN when absolutely necessary.
- **Don't share personal information** (birthdate, Social Security number, or bank account number) just because someone asks for it.
- Collect mail every day. **Place a hold on your mail when you are away** from home for several days.
- Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
- Use the **security features on your mobile phone.**
- **Update sharing and firewall settings** when you're on a public wi-fi network. Use a virtual private network, if you use public wi-fi.
- **Review your credit card and bank account statements**. Compare receipts with account statements. Watch for unauthorized transactions.
- **Shred receipts, credit offers, account statements,** and expired credit cards, to prevent "dumpster divers" from getting your personal information.
- **Store personal information in a safe place.**
- Install firewalls and virus-detection software on your home computer.
- **Create complex passwords** that identity thieves cannot guess. Change your passwords if a company that you do business with has a breach of its databases
- **Review your credit reports once a year.** Be certain that they don't include accounts that you have not opened. You can order it for free from Annualcreditreport.com.
- **Freeze your credit files with Equifax, Experian, Innovis, TransUnion,** and the National Consumer Telecommunications and Utilities Exchange for free. Credit freezes prevent someone from applying for and getting approval for credit account or utility services in your name.

LegalShield® BUSINESS SOLUTIONS

Report Identity Theft

Report identity (ID) theft to the Federal Trade Commission (FTC) online at IdentityTheft.gov or by phone at 1-877-438-4338.

The Equifax breach is a stark reminder that forces beyond your control can lead to the exposure of your personal information. **It's an important reminder that everyone needs identity theft protection**. 148 Million Americans are affected and at risk for identity theft (about 44% of the population)! The personal information that was exposed includes the following:

- You Full Name
- Social Security numbers: We already are acutely aware of the effects from this form of breach.
- Date of Birth
- Addresses
- **Driver's License: This is the big one as a theft can use your driver's license as an official document.**
- Credit Cards

LegalShield®
BUSINESS SOLUTIONS

LegalShield®

Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

START QUIZ >

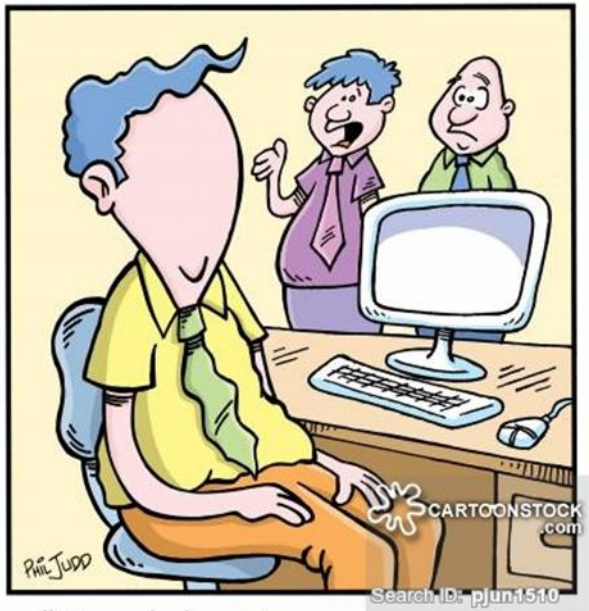
LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 1

How much financial loss is due to personal identity theft every year?

- $5 million
- $200 million
- $4.2 billion
- $24.7 billion



"Frank has been a victim of identity theft!"

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 1

How much financial loss is due to personal identity theft every year?

- $5 million
- $200 million
- $4.2 billion
- X $24.7 billion

ANSWER

$24.7 billion

The Bureau of Justice Statistics found that financial losses due to personal identity theft totaled $24.7 billion in 2012.[1]

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 2

How many people fall victim to Identity Theft every year?

- 10,000
- 100,000
- 1 million
- 10 million

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 2

How many people fall victim to Identity Theft every year?

- 10,000
- 100,000
- 1 million
- X 10 million

ANSWER

10 Million

The number of annual identity theft victims is well above 10 million. In 2013, 13 million individuals experienced some form of identity Theft.[1] In 2012 it was as high as 16.1 million[2]

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 3

Which of these methods ARE NOT used by identity thieves to gain access to passwords and other personal information?

- Cloned website
- Keyloggers
- DDoS attacks
- Rummaging through your trash
- Skimming devices

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 3

Which of these methods ARE NOT used by identity thieves to gain access to passwords and other personal information?

- Cloned website
- Keyloggers
- X DDoS attacks
- Rummaging through your trash
- Skimming devices

ANSWER

Direct Denial of Service (DDoS) attacks

DDoS attacks are not used to steal information, they are attacks that crash webservers. Identity Thieves attempt to access your information by creating fake websites, keylogging programs designed to capture your keystrokes, digging through your trash and skimming devices used to steal payment card data.

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 4

What is phishing?

- Someone creates an official form of government ID in your name.
- When thieves look through your garbage in hopes to find personal information.
- A scam designed to trick a person into divulging personal information.
- Your identity is stolen while at a concert or sporting event

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 4

What is phishing?

- ○ Someone creates an offi
  government ID in your nam
- ○ When thieves look throu
  in hopes to find personal in
- X A scam designed to trick a person into divulging personal information.
- ○ Your identity is stolen while at a concert or sporting event

ANSWER

Phishing

Phishing is when thieves trick victims into sharing personal financial information (such as bank accounts, passwords and Social Security numbers) voluntarily.

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 5

What was the most common form of ID theft in 2013?

- Government Documents/ Benefits Fraud
- Credit Card Fraud
- Utilities Fraud
- Bank Fraud
- Employment Related Fraud
- Loan Fraud

LegalShield
Worry Less. Live More.

WHAT'S YOUR IDENTITY THEFT IQ?

QUESTION 5

What was the most common form of ID theft in 2013?

- [x] Government Documents/ Benefits Fraud
- [ ] Credit Card Fraud
- [ ] Utilities Fraud
- [ ] Bank Fraud
- [ ] Employment Related Fraud
- [ ] Loan Fraud

ANSWER

Government Documents / Benefits Fraud

The FTC found that 34% of identity theft in 2013 was Government Documents/Benefits Fraud. Credit Card Fraud was a close second at 17%.[1]

Increase Your Identity Theft IQ!

LegalShield® BUSINESS SOLUTIONS

What is Identity Theft?

- Financial
- Social Security
- Medical
- Character
- Social Security
- Tax Fraud
- Government Docs
- Insurance
- Driver's License

LegalShield®
BUSINESS SOLUTIONS

Identity Theft Protection

- Resolution
- Reimbursement
- Restoration

LegalShield®
BUSINESS SOLUTIONS

Resolution - Good

- Offers “Help” to restore your Identity
- Gives access to Identity Theft counselors to assist you in restoring your Identity
- Will give consultation on who to contact, how to fill out forms, and where to obtain forms to fill out to begin restoration process
- Oftentimes, a free value-added service to an insurance plan or EAP

LegalShield®
BUSINESS SOLUTIONS

Reimbursement - Better

- Gives access to Identity Theft counselors to assist you in restoring your Identity
- Many times comes with credit monitoring
- Will give consultation on who to contact, how to fill out forms, and where to obtain forms to fill out to begin restoration process
- Will reimburse you up to certain limitations for money spent in the restoration process (Does NOT reimburse losses due to Identity Theft, but does reimburse money spent in the restoration process up to category limits).
- An underwriter will determine what expenses in the restoration process will be reimbursed.
- Costs can average $8 - $10 per person

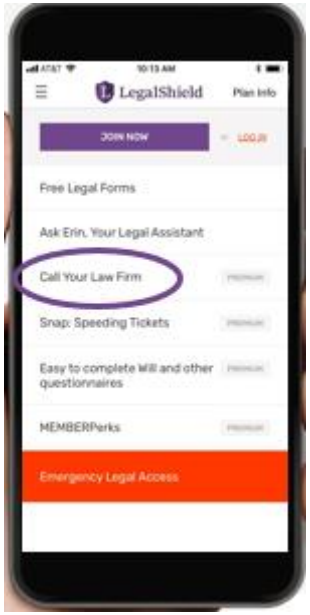
LegalShield® BUSINESS SOLUTIONS

Restoration - Best

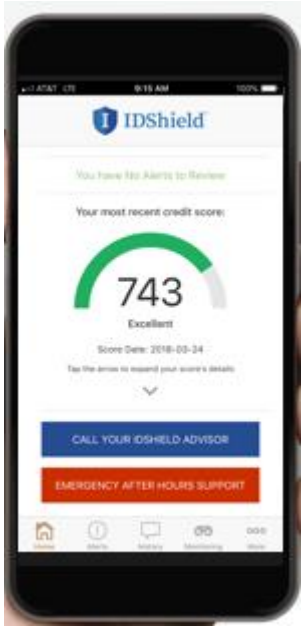
- Gives access to Identity Theft counselors questions about Identity Theft.
- Usually comes with Daily Credit Monitoring
- In the event of Identity Theft, the company will give you the option for complete restoration, covered by the plan (not reimbursed).
- Depending on the company, you may be outsourced to an unknown 3rd Party for this restoration or you may have access to a dedicated Risk Management expert for these services (check with your plan provider for details).
- Full Restoration Plans can range from $10 - $15 per person

LegalShield® BUSINESS SOLUTIONS

LegalShield℠ | IDShield℠



- Affordable
- Convenient
- Accessible
- Responsive



Questions?

LegalShield®
BUSINESS SOLUTIONS

Thank You

LegalShield

The information contained in this material is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the coverage you have selected. Please remember that only the plan contract can give actual terms, coverage, amounts, conditions, and exclusions. Check benefit availability in your state/province.

Marketed by Pre-Paid Legal Services, Inc. dba LegalShield or applicable subsidiary:
Pre-Paid Legal Casualty[SM], Inc.
In Florida: Pre-Paid Legal Services, Inc., of Florida
In Virginia: Legal Service Plans of Virginia, Inc.
Pre-Paid Legal Access, Inc.
PPL Legal Care of Canada, Inc.

LegalShield®
BUSINESS SOLUTIONS