RESTECH SOLUTIONS

MOHTHLY ILLUMINATIONS

LIGHTING THE DARK WEB℠
APRIL 2020

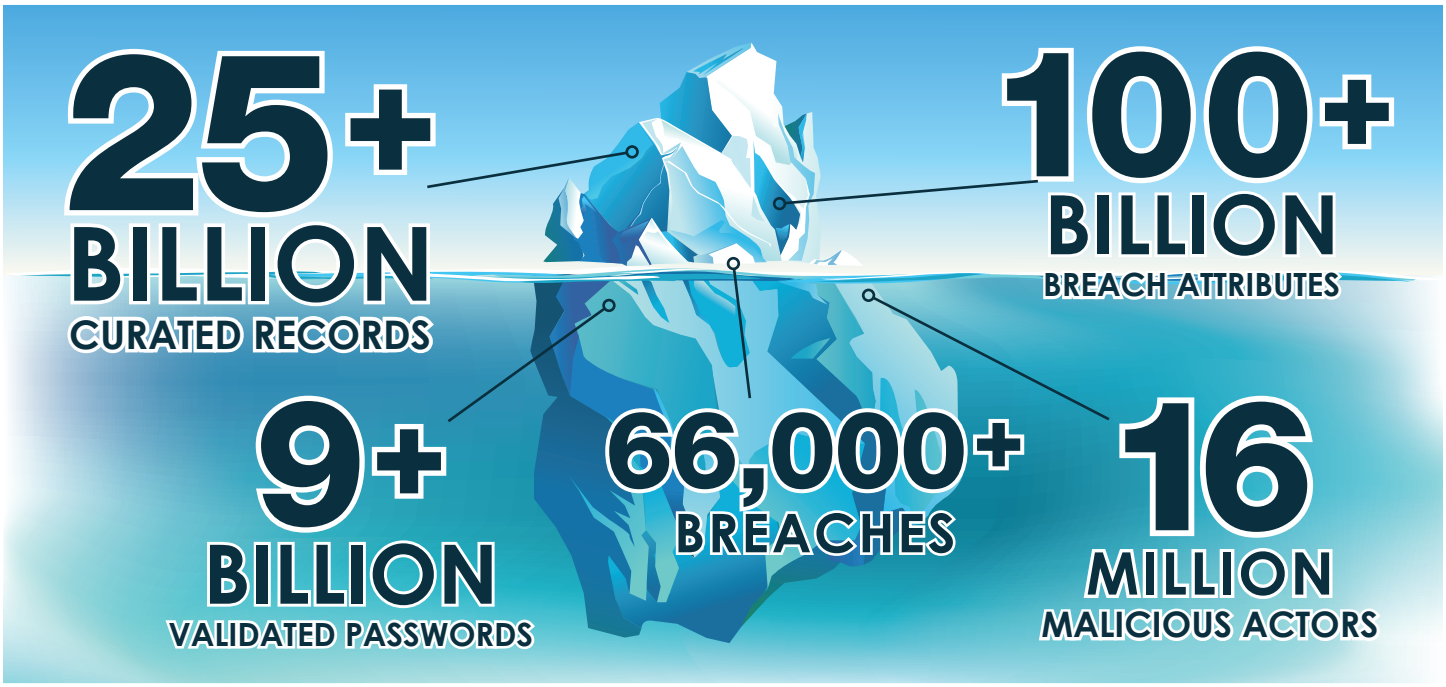
ResTech Solutions
Solutions for a Human World

CONTENTS

Disclaimer
The information in this report has been prepared to alert potentially affected parties of exposed data that may be publicly available using online resources. ResTech Solutions does not make any representations, warranties or guarantees with respect to the completeness or accuracy of the reported exposures or any other information in this report.

1. INTRODUCTION

In the last few years we have seen an increase in the number of incidents and data breaches. Hackers, organized crime, and nation sponsored attacks around the world have resulted in a surge of stolen data being sold in the black market. Billions of usernames, passwords, and terabytes of documents have been exposed in the deep and dark web. ResTech Solutions monitors the surface, social, deep and dark web detecting exposed identities and stolen data helping consumers and companies manage the risk.



WHAT IS AN INCIDENT?

ResTech Solutions defines an incident as when a company has a vulnerability but there is no confirmation of whether anything was stolen.

WHAT IS A DATA BREACH?

ResTech Solutions defines a data breach as a confirmed incident where credentials, personal, medical and/or financial records or other sensitive data have been accessed or disclosed due to being hacked or leaked, either accidentally or on purpose.

WHAT IS ACCIDENTAL EXPOSURE?

ResTech Solutions defines an accidental exposure as a type of data breach that can be attributed to human error or inadequate security measures. Examples range from default or misconfigurations of anonymous FTPs and cloud-based databases (e.g. MongoDB) to lost laptops, tablets or mobile phones that contain or provide access to sensitive information.

2. REPORT CONTENT

All of the data breach information used in this report has been aggregated from the ResTech Solutions database between **March 1st to March 31th, 2020**. The following tables represent how the information has been classified depending on the data types.

All data has been extracted before the normalization and data accuracy analysis so the information shown in this report could vary.

Each entry has been analyzed to determine the record types compromised.

STATISTICS

The total number of exposed identities in the month:	
RAW IDENTITY RECORDS	
Period	Number
March 2020	**233,496,218**

The total number of breaches found in the month:	
NEW BREACHES FOUND	
Period	Number
March 2020	**547**

The total number of exposed identities after cleaning duplicates and fake data:	
CLEANSED IDENTITIES	
Period	Number
March 2020	**167,668,814**
**Note: Due that combo lists are created using parts from other breaches, they are not included in this table*	

Number of exposed identities by each type of breach (raw–not cleansed):	
CLEANSED IDENTITIES	
Type	Number
Marketing / Aggregated	**63,168,741**
Leaked/Unknown	**44,883,923**
Hacked	**22,781,742**
Combo Breaches	**65,827,404**
Voters	**36,834,408**

3. STATISTICS CHART

3.1 Monthly Breaches - Data Distribution

(March 2019)

This chart shows the total number of records by exposed fields in the monthly breaches coming from cleansed identities:

139,764,305
EMAIL

32,985,688
PASSWORD

4,740,360
SALT

10,759,215
USERNAME

9,783,026
IP ADDRESS

147,984,059
NAME

33,992,724
BIRTHDATE

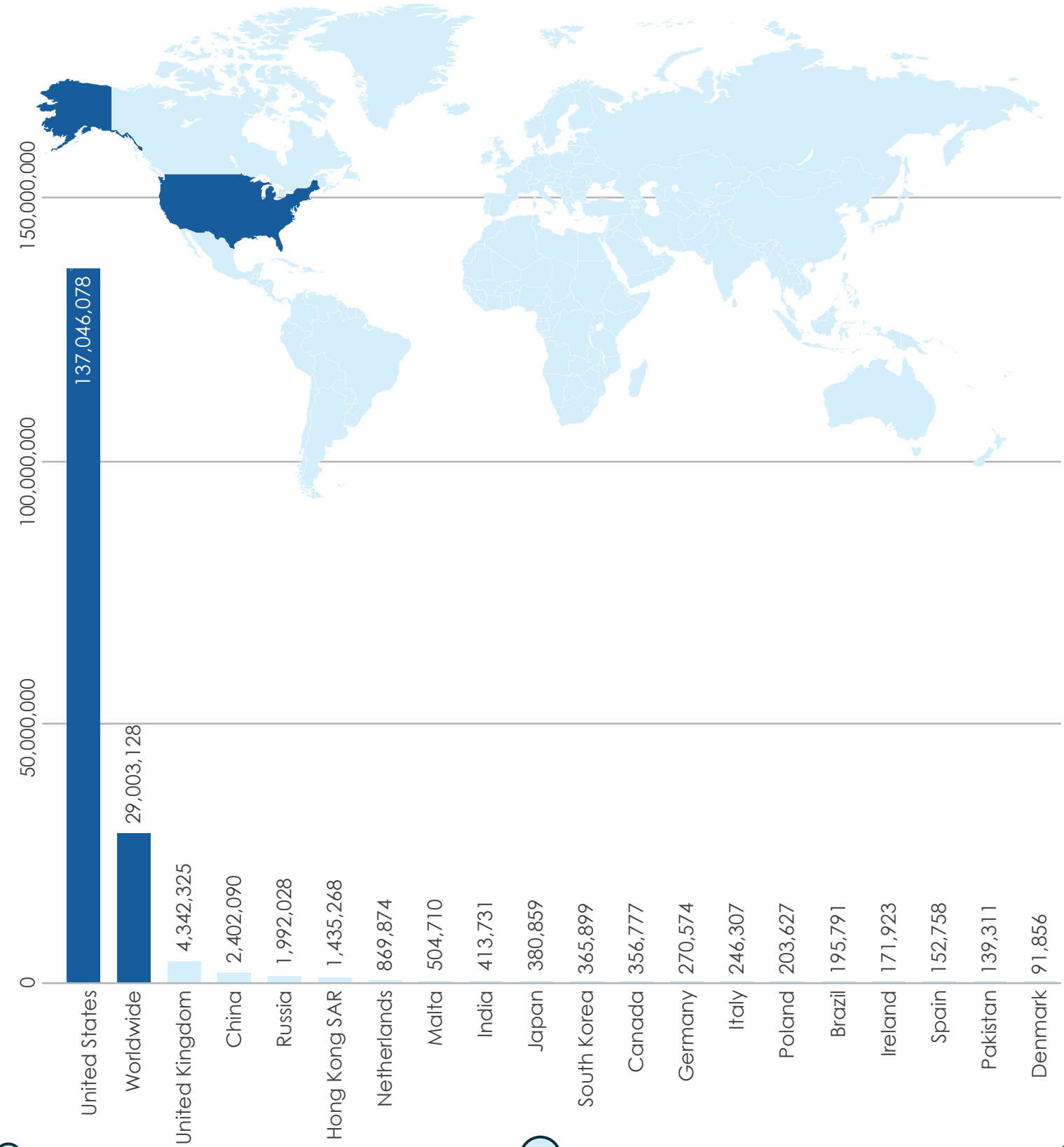
127,537,425
PHONE NUMBER

147,599,303
BIRTHDATE

30,384,866
SOCIAL

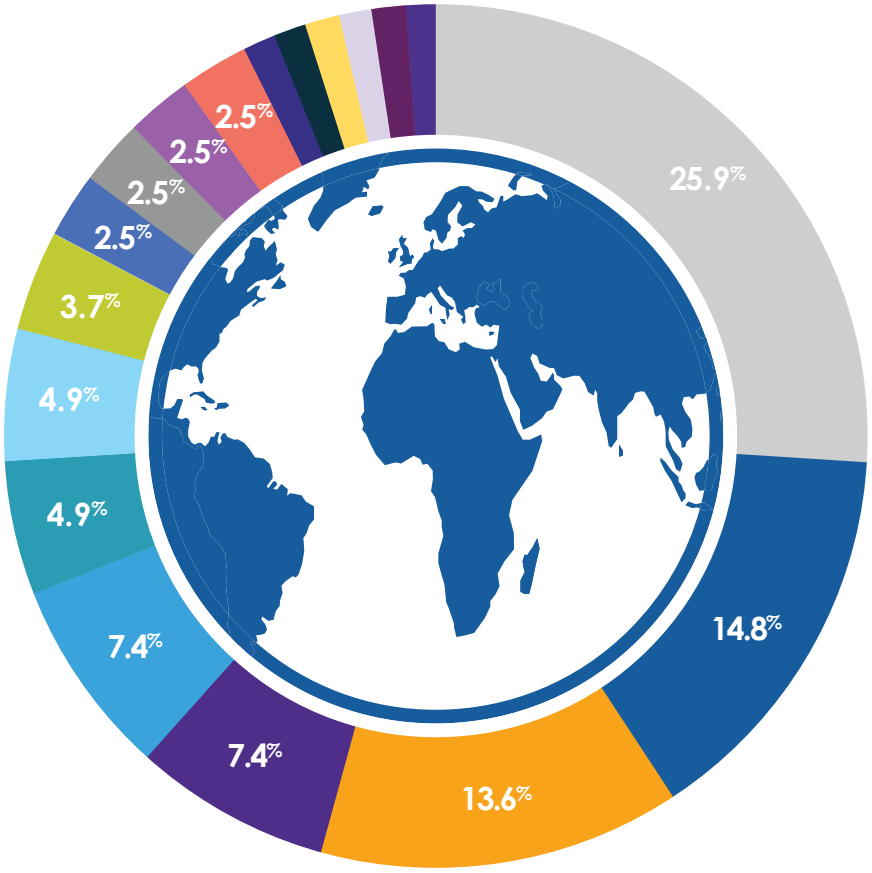
3.2 Geographic Distribution Of Breaches (March 2019)

The following map represents the total number of breaches reported during **March 2020** geographically coming from cleansed identities:



3.3 DISTRIBUTION OF INCIDENTS BY CATEGORY (March 2020)

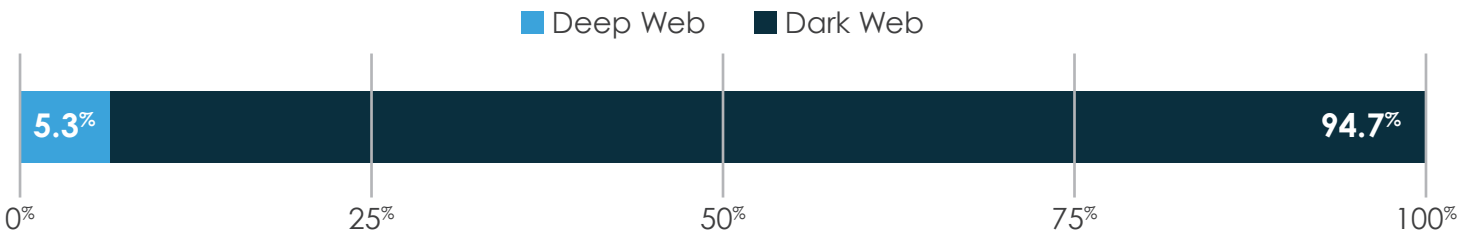
The following chart represents the percentage of breaches reported during **March 2020** by its category coming from cleansed identities:



- Others 25.9%
- Gaming 14.8%
- Voters13.6%
- E-Commerce 7.4%
- Service Providers 7.4%
- Forum 4.9%
- Academic 4.9%
- Social Media 3.7%
- Employment Services 2.5%
- Gambling 2.5%
- File Sharing 2.5%
- Crypto Currency 2.5%
- Adult 1.2%
- Healthcare 1.2%
- Sport 1.2%
- Business 1.2%
- Hosting1.2%
- News1.2%

3.4 DISTRIBUTION OF INCIDENTS BY SOURCE OF THE INFORMATION (March 2020)

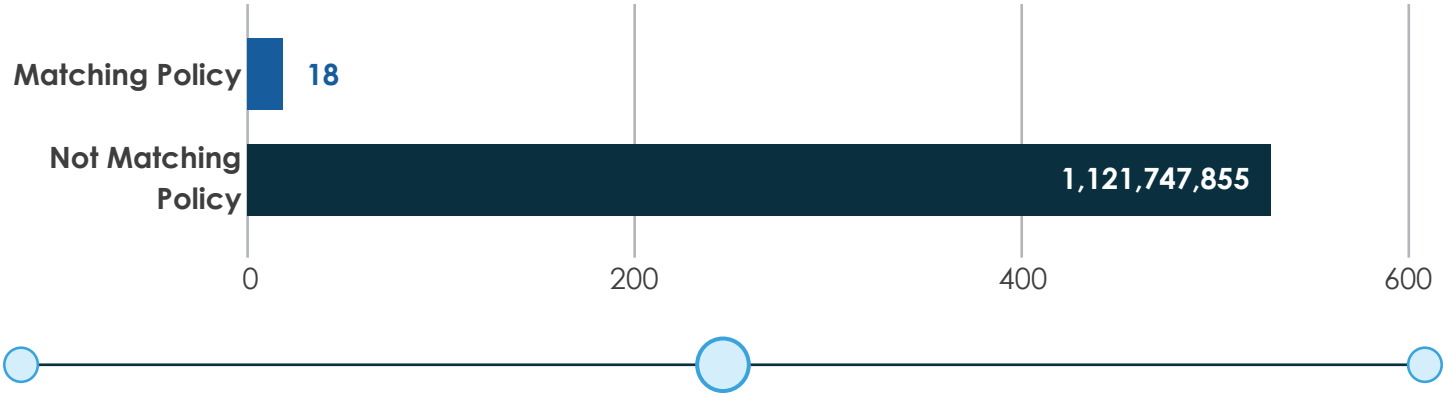
The following chart represents the percentage of breaches reported during **March 2020** by its source:



3.5 NUMBER OF BREACHES MATCHING LIFELOCK POLICY (March 2020)

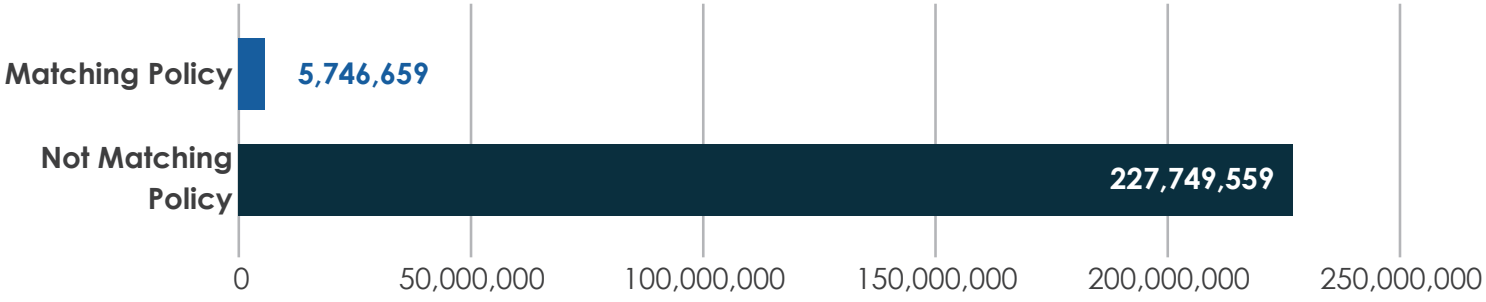
Since Lifelock is not sending a number of alert types to their customers (phishing, marketing, aggregators, combos) only a percentage of the breaches are used for alerts.

These charts show the comparison between the number of breaches matching Lifelock policy and the breaches not matching policy.



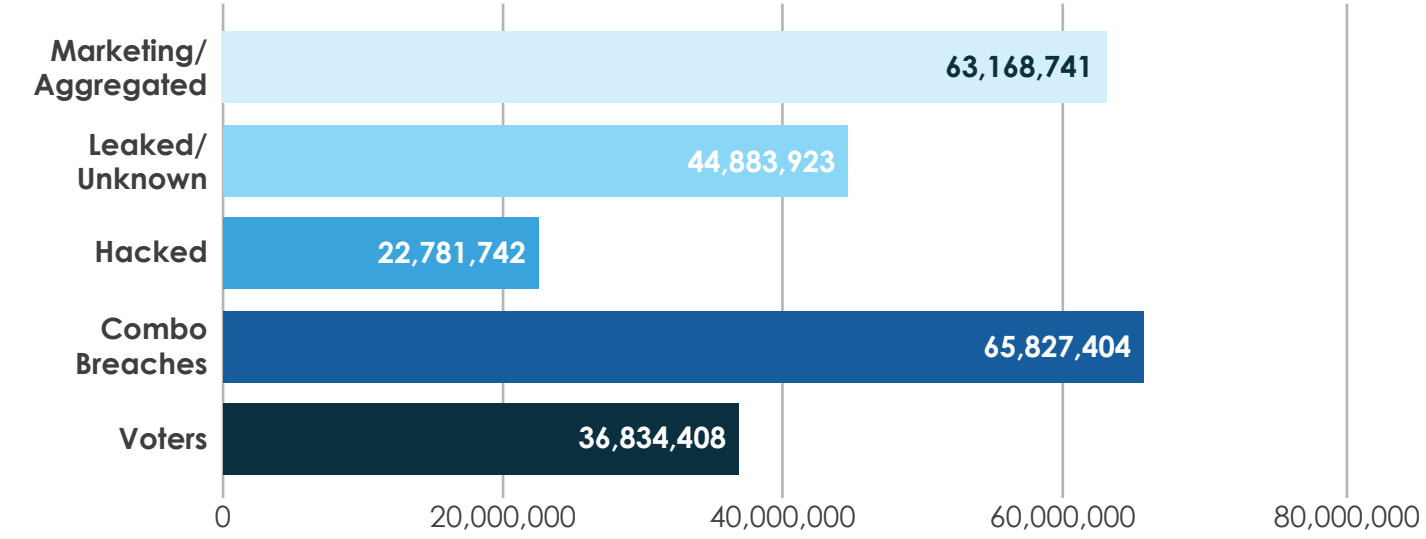
3.6 NUMBER OF IDENTITIES EXPOSED MATCHING LIFELOCK POLICY (March 2020)

These charts show the comparison between the number of identities from breaches that match Lifelock policy and the identities non matching policy.



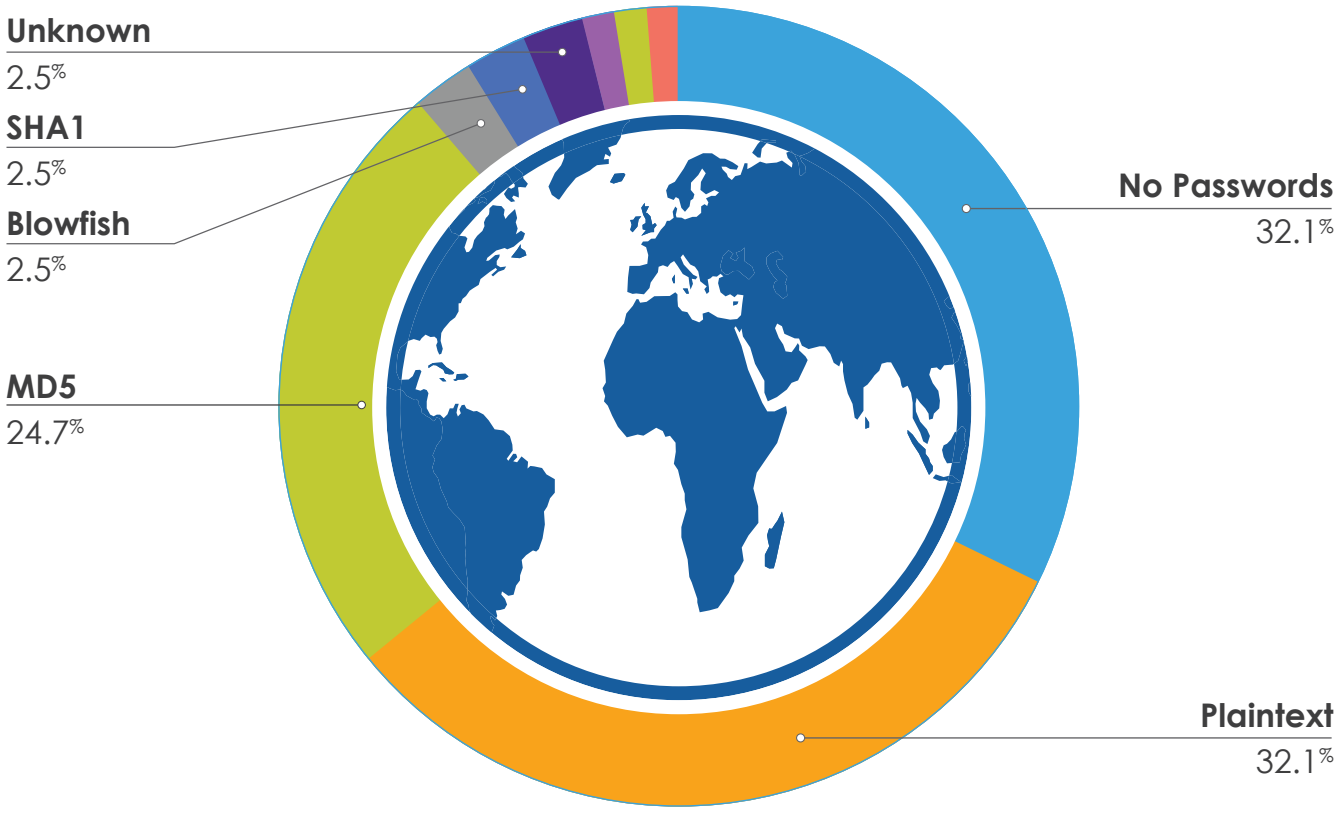
3.7 NUMBER OF IDENTITIES EXPOSED BY TYPE (March 2020)

The following chart represents the number of identities detected during **March 2020** by its type:



3.8 DISTRIBUTION OF INCIDENTS BY PASSWORD ENCRYPTION TYPE (March 2020)

The following chart represents the percentage of breaches reported during **March 2020** by its type of encryption coming from cleansed identities:



4. TOP FEATURED BREACHES/ INCIDENTS DETECTED

The top incidents reported in the month of March 2020 are:

TOP BREACHES FROM MARCH 1ST TO MARCH 31ST, 2020	
BREACH NAME	**DESCRIPTION**
insanityflyff.com	The site insanityflyff.com has been reported in March 2020 to possibly have suffered a data exposure that could include 2,229,469 emails and passwords.
salesforce.com	The site salesforce.com has been reported in March 2020 to possibly have suffered a data exposure that could include 2,173,699 names, surnames, and addresses.
ccidnet.com	The site ccidnet.com has been reported to possibly have suffered a data exposure that could include 1,762,103 usernames, emails, passwords and IP addresses. The possible exposure would have happened in December 2013 although it was reported in March 2020.
dejhiodjw.com	The site dejhiodjw.com has been reported in March 2020 to possibly have suffered a data exposure that could include 1,369,697 emails and passwords.
oxmc.ru	The site foxmc.ru has been reported to possibly have suffered a data exposure that could include 1,252,996 usernames, passwords and IP addresses. The possible exposure would have happened in March 2018 although it was reported in March 2020.

ABOUT RESTECH SOLUTIONS

ResTech Solutions protects identities and companies by scanning the surface, social and deep and dark web for stolen, leaked or lost login credentials and other information.

ResTech Solutions helps organizations measure, monitor and manage digital risk by identifying network users with stolen credentials, the single greats source of cybercrime on the dark web.

ResTech Solutions notifies organizations and individuals in real time when credentials first appear to guard against the theft of identities, information and money before it happens. We are strong advocates of effective password security protocols as outlined by the National Institute of Standards and Technology (NIST) and embrace their Cybersecurity Framework throughout our company, and in the execution of our services.

RESTECH
SOLUTIONS

ILLUMINATING THE DARK WEB[SM]

ResTech Solutions Headquarters
8715 Meadowcroft Dr. #102
Houston, TX 77063

www.restech.solutions