RESTECH SOLUTIONS

THE CHANGING LANDSCAPE OF IDENTITIES IN THE WILD

THE LONG TAIL OF SMALL BREACHES

2019 ResTech Solutions Identity Breach Report

CONTENTS

1. INTRODUCTION

In 2018, ResTech Solutions observed a significant shift from attacks on not just large companies, but increasing attacks on a greater number of small businesses – the long tail – as hackers targeted unsophisticated and unsecured small businesses and supply chain vendors. There was also an increase in large volumes of repackaged and shared stolen passwords, as well as the continuation of 2017's trend of openly leaking devices. 2018 saw an increase of open or publicly exposed personal identifiable information (PII) – including voter records and government databases – being packaged for malicious or criminal activity. In this report, ResTech Solutions describes 2018 trends and the changing landscape of stolen identities.

RESTECH SOLUTIONS SAW

14

BILLION

IDENTITY RECORDS

circulating, with **3.6 Billion New, Authentic Identity Records in 2018**

RESTECH SOLUTIONS CONFIRMED

12,449

REAL, NEW IDENTITY BREACHES

(More than **four times** as many as 2017)

When thinking about big data breaches, companies like Yahoo, Equifax, Anthem, and Target are often the first that come to mind. Following a similar pattern, 2018 saw companies like Google, Facebook, and Marriott make headlines as well. With new breaches being reported on an almost daily basis, "breach fatigue" has set in, with their occurrence becoming the "new normal."

Historically, large companies with vast quantities of data have been the prime targets for data breaches. With a single hack, bad actors are able to exfiltrate data on millions of consumers which can then be used to launch other attacks or sold to other cyber criminals for malicious purposes such as identity theft, fraud, and account takeover.

2018 saw continued investment in cyber security with better protection for large companies. The General Data Protection Regulation (GDPR) raised awareness not just in Europe, but also in boardrooms in the US and across the world. With serious penalties for non-compliance, IT teams, business risk managers and the lines of business reviewed their data collection and retention policies and put more processes and systems in place to safeguard data assets.

While these investments may result in improving the security posture of enterprises, small businesses and suppliers for large companies present weak links in the value chain–they have little to no cybersecurity budgets and are far less able to secure themselves from increasingly organized hackers who are systematically targeting them. Not surprisingly, in 2018, we saw a significant increase in the number of attacks on small entities.

As large firms are increasing their levels of sophistication, so too are hackers and cyber criminals. They have become more organized and well-funded, improving their operational and scaling capabilities while advancing their methods for aggregating new data sets.

One emerging trend has been to combine open and publicly available data sources with leaked or stolen data to better profile individuals.

Bad actors are building, packaging and selling databases of consumer data with personal identifiable information (PII). They are combining stolen identity attributes (email addresses, passwords, passport numbers, healthcare records, prescription purchases, insurance information, travel or geo-location data, shopping habits, political views, and more) with public records (name, date of birth, home address, etc.), making it easier for criminals to launch new attacks involving account takeover, identity theft, fake email fraud, or other forms of social engineering.

2018 also saw hackers assembling bigger combo password lists that aggregate clear text credentials from hundreds of breaches. Each time a combo password collection is repackaged, new credentials are added to increase the total size, and each new package fuels renewed credential stuffing and account takeover attempts. Combo Lists containing 1.82 billion credentials resurfaced throughout 2018 and in early 2019.

2018 saw voter records, citizen identity information, and government data being increasingly targeted and traded in underground communities. This trend relates to growing geopolitical tensions and state sponsored attacks. The government sector saw the largest increase in breaches across all breached industries in 2018.

At the same time, law enforcement agencies (LEAs) are becoming more knowledgeable with respect to tracking cyber criminals and taking down darknet marketplaces. In 2018, cyber criminals were forced to move away from trading in large markets to smaller, more decentralized channels: forums, private communities, and data brokers who specialize in stolen data.

These trends and the continued proliferation of openly leaking devices are the major themes of the **2019 Identity Breach Report: The Changing Landscape of Breach Identities**.

2. ABOUT THIS REPORT

This report is based on breaches and leaks found in 2018. In addition to breaches reported in the media, ResTech Solutions detects information found in data dumps posted in open, but often transient, sources in the deep and dark web. Many of these breach corpuses are not known to the general public.

ResTech Solutions' automated crawlers and subject matter experts use a variety of sources to authenticate and verify the data, including:

- The surface web
- Social media
- Underground communities and forums
- Black markets
- The deep web
- The dark web

Then, ResTech Solutions analyzes, verifies, normalizes, cleans, and attributes the data to further understand the severity of risks facing consumers and companies. Finally, we alert the impacted parties in order to mitigate risks. ResTech Solutions assesses the severity of risk based upon multiple factors:

- Sensitivity of information
- Authenticity of the data
- Number of individuals impacted
- How old the data is for each type of sensitive identity attribute exposed

3. 2018 INSIGHTS

In 2018, criminals shifted their focus from large corporations to **SMALL BUSINESSES**, resulting in the discovery of almost four times as many breaches than in 2017.

12,449

NEW, AUTHENTIC BREACHES & LEAKS IN 2018

424% increase from in 2017

The **average breach size** in 2018 was **216,884 records – 4.7 times smaller** than the year before. This is a direct result of the trend of the increasing number of small breaches.

As hackers increase their sophistication with new hacking tools, they are better able to attack larger numbers of small businesses. Targets that cyber criminals would have previously deemed too small to spend time attempting to infiltrate are now at risk.

IDENTITY BASED CRIMINAL ACTIVITY continues to grow at an exponential rate.

14.9 billion raw identity records circulated across the web. This is a significant increase from last year's **8.7 billion**. After analyzing, normalizing, and cleansing the data, around **3.6 billion** of this year's records were real (not fake) and new. This is 20% higher than 2017's **3 billion curated identity records**, and illustrates the increasing use of identity information for criminal activity, such as account takeover, business email compromise, identity theft, and other attacks.

71%

INCREASE IN UNDERGROUND ACTIVITY IN 2018

CITIZEN DATA is being targeted for Geopolitical purposes in the new Cyber Cold War.

In 2018, the government sector number of identity exposures had a significant increase **291%** (see 5.7). For the first time we saw underground brokers actively including citizen data, such as voter databases, as part of their data portfolio. The heightened interest in public records is related to geopolitical tensions, the cyber cold war, and election manipulation campaigns. As an example, in 2018, numerous dumps from the US, China, and Russia exposed citizen data, voter records, as well as, financial and customer databases. **ResTech Solutions will expand on this topic in a future report**.

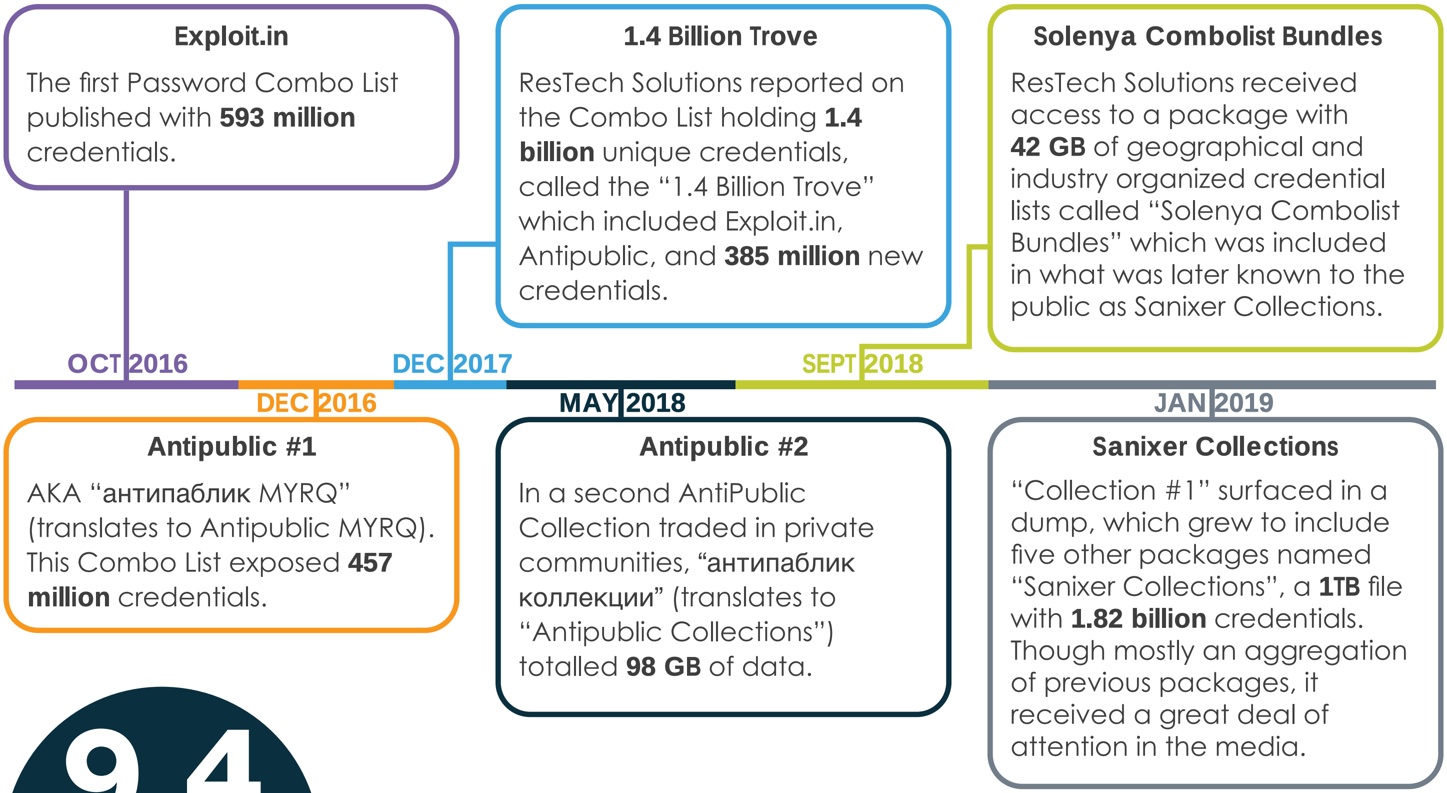
MASSIVE PASSWORD COMBO LISTS continue to grow to support account takeover campaigns.

1.8 BILLION
CLEAR TEXT CREDENTIALS AGGREGATED INTO ONE SINGLE PACKAGE

The circulation and repackaging of username and password databases into "Combo Lists" has seen a sharp increase in 2018.

These lists with clear text passwords from thousands of breaches are being aggregated and repackaged, creating a snowball effect.

The data is used to automate brute-forcing of authentication on websites, taking advantage of the fact that people reuse passwords across many sites. A number of open source tools automate the testing of these username and password combinations for 'account takeover', a major problem that persists in cyber security today.



OCT 2016

Exploit.in

The first Password Combo List published with **593 million** credentials.

DEC 2016

Antipublic #1

AKA "**антипаблик** MYRQ" (translates to Antipublic MYRQ). This Combo List exposed **457 million** credentials.

DEC 2017

1.4 Billion Trove

ResTech Solutions reported on the Combo List holding **1.4 billion** unique credentials, called the "1.4 Billion Trove" which included Exploit.in, Antipublic, and **385 million** new credentials.

MAY 2018

Antipublic #2

In a second AntiPublic Collection traded in private communities, "**антипаблик коллекции**" (translates to "Antipublic Collections") totalled **98 GB** of data.

SEPT 2018

Solenya Combolist Bundles

ResTech Solutions received access to a package with **42 GB** of geographical and industry organized credential lists called "Solenya Combolist Bundles" which was included in what was later known to the public as Sanixer Collections.

JAN 2019

Sanixer Collections

"Collection #1" surfaced in a dump, which grew to include five other packages named "Sanixer Collections", a **1TB** file with **1.82 billion** credentials. Though mostly an aggregation of previous packages, it received a great deal of attention in the media.

9.4 BILLION
TOTAL RAW IDENTITY RECORDS IN 2018
88% INCREASE OVER 2017

ACCIDENTAL EXPOSURES from open devices accounted for three of the year's largest breaches, but the number of leaking devices showed a slow decline.

As ResTech Solutions predicted in 2017, 2018 was a record year for breaches caused by open devices, with a much larger number of accidental exposures than exposures due to hacking. Many companies migrating to the cloud accidentally left their databases and servers open. Organized adversaries are using automated crawlers to detect open devices and exfiltrate leaking data.

WHERE IDENTITY RECORDS WERE FOUND

37% Underground **63%** Accidental

4. TOP 12 BREACHES OF 2018

A leaderboard of the year's breaches in terms of size and importance of exposed data presents more insight into the changing landscape of breached identities in 2018. Topping the list is the Anti Public Combo Collection, an aggregation of clear text usernames and passwords, that hackers use to launch credential stuffing and account takeover attacks. Although Anti Public was publicly disclosed in January of 2019, most of the data was repackaged and re-circulated in a variety of surface, deep and dark web sources throughout 2018. Not all of these top 12 breaches have been seen in open sources to date

BREACH NAME	DESCRIPTION
1. **Anti-Public Combo Collections**	**2018 - 2019 – (HACKED, COMBO PACKAGE)** The Anti Public Combo Collection, (a.k.a. Sanixer Collection #1-6 made headlines in 2019, but most of the data was leaked in 2018. The package contains 95% of the data in **Sanixer** and includes two Anti Public lists and the **Solenya** Combo-list Bundle, making it a total of seven packages. The Collection was originally **562 MILLION** records but grew to **30 BILLION** raw (many duplicated, old) records, with only **1.8 BILLION** unique email addresses.
2. **Aadhaar, India**	**March 2018 – (OPEN DEVICE, 3RD PARTY BREACH)** State-owned utility company Indane neglected to secure an API. This left open access to India's Government ID database of citizens' identity and biometric info. **1.1 BILLION** Indian citizens were affected and the exposed data included **names**, **12-digit ID numbers**, **postal codes (PIN)**, **photos**, **phone numbers**, **emails**, and **information on connected services such as bank accounts**. Hackers put Aadhaar card details on sale for Rs 500 and used WhatsApp to reach potential buyers.
3. **Marriott Starwood Hotels**	**September 2018 – (HACKED)** Hackers accessed the Starwood hotel chain reservation database and stole information on **500 MILLION** guests, including their **phone numbers**, **email addresses**, **passport numbers**, r**eservation dates**, **payment card numbers**, and **expiration dates**. This hack was part of a larger move against American companies by China-based hackers. The vulnerability resided in the Starwood hotel systems, providing a weak link in Marriott's security infrastructure post acquisition.
4. **Exactis**	**June 2018 – (OPEN DEVICE)** A security expert discovered the marketing company's database on an open, publicly accessible server leaking PII (**phone numbers**, **addresses**, **personal interests**, and more) of **340 MILLION** people and businesses.
5. **HuaZhu Group**	**August 2018 – (ACCIDENTAL EXPOSURE)** Over **130 MILLION** customers' personally identifiable information was hacked from a large Chinese hotel conglomerate and posted for sale on a Chinese dark web forum in a three part collection. Leaked information includes over **240 MILLION** lines of data, including **phone numbers**, **email addresses**, **bank account numbers**, and **booking details**. The breach was a result of the hotel group's software developers accidentally uploading a database to Github.

BREACH NAME	DESCRIPTION
6. Apollo	**February 2018 – (OPEN DEVICE)** This “sales engagement” database was accessed by an “unauthorized party,” exposing the **usernames** and **emails** of **150 MILLION** app users. ResTech Solutions records show additional fields exposed include **email addresses**, **employers**, **geographic locations**, **job titles**, **names**, **phone numbers**, and **social media profiles**.
7. Quora	**November 2018 – (HACKED)** A “malicious third party” accessed Quora’s system, stealing account information for **100 MILLION** users, including their names, emails, encrypted **passwords**, **data from accounts linked to Quora**, and **users’ public questions and answers**. Unlike many packages that are sold for high volume at low prices, this valuable data set was available for sale privately to a select group of buyers and commanded a relatively high price.
8. Google+	**2015 - 2018, November 7 - 13, 2018 – (API GLITCH)** First reports indicated a Google+ software glitch exposing personal profiles of 500k Google+ users. Then, in December, a second API bug exposed **52.5 MILLION** users. Exposed PII includes **user names**, **emails**, **employers**, **job titles**, **birthdates**, **ages**, and **relationship statuses**. To date, ResTech Solutions has not.
9. Chegg	**April 29 - September 19, 2018 – (HACKED)** An “unauthorized party” gained access to education technology company Chegg’s user database for chegg.com, along with user data from the Company’s family brands such as EasyBib, exposing **40 MILLION** accounts with **names**, **emails**, **addresses**, **shipping addresses**, **account usernames**, and **passwords**. ResTech Solutions SMEs found this data and verified the information.
10. Cathay Pacific Airways	**March 2018 – (SOPHISTICATED TARGETED ATTACK)** This breach was reportedly carried out by sophisticated hackers who attacked the company’s database over the course of five months. Data on 9.4 MILLION passengers was exposed, including 860k passport numbers, 245,000 Hong Kong ID card numbers, 403 expired credit card numbers, and 27 credit card numbers (without CVV).
11. Shein	**June 2018 – (HACKED)** This women’s fashion and e-commerce site was hacked, and data (emails, encrypted passwords, and more) on at least **6.4 MILLION** consumers was exposed. ResTech Solutions discovered the breach, issued notifications, and received confirmation from the company as part of it’s responsible disclosure policy.
12. Facebook	**July 2017 - 2018 – (API GLITCH)** Unknown hackers exploited a glitch in Facebook’s code and retrieved access tokens for at least **4.6 MILLION** consumers, allowing them to scrape compromised user accounts and collect highly sensitive data, including **locations**, **contact details**, **relationship statuses**, **recent searches**, and **devices used to log in**.

5. DATA VERIFICATION

5.1 RESTECH SOLUTIONS CURATION PROCESS: VALIDATING REAL AND UNIQUE IDENTITIES EXPOSED

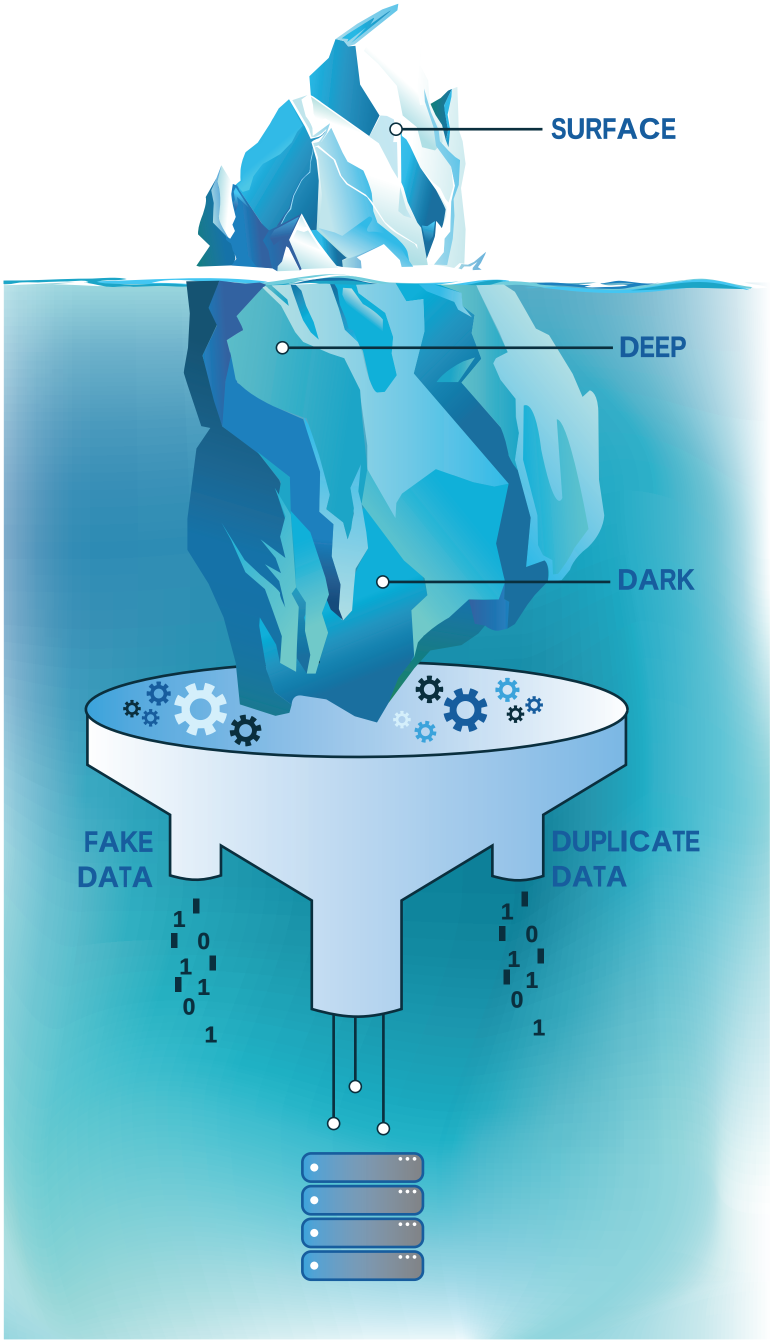
While the number of accumulated raw identity records provides insight into the sheer volume of data points out there, it is not the best indicator of overall risk.

This is because not all of the data gathered is authentic or unique.

After gathering the raw data, the next step is to analyze the details. ResTech Solutions uses machine learning algorithms which quickly identify real (not fake) data, flag sensitive data and remove duplicate records.

Next, breaches undergo a verification process, during which our analysts and experts use numerous research and investigative methods to ensure that the domain and other breach information is real and valid. The breach is then attributed and normalized.

After a breach is verified, the ResTech Solutions platform calculates a risk score based on a number of variables such as types of attributes, date, and strength of password.



5.2 CURATED BREACHES IN 2018

In 2018, ResTech Solutions analyzed tens of thousands of "breach corpuses" and found that 12,449 of them were authentic. The others were either fake or duplicates from other breaches. This is equivalent to 1,037 breaches every month, or 34 breaches every day.

The number of breaches is significantly higher than in 2017, which saw 3,535 "breach corpuses" with 2,940 of them being authentic. This means that 2018 saw a 424% increase in breaches exposed from the year before. The curated data revealed that identity records from these 12,449 breaches were all available to bad actors at some point throughout the year.

12,449
TOTAL BREACHES IN 2018

1,037
EVERY MONTH

34
EVERY DAY

5.3 NEW VALIDATED IDENTITIES FOUND EXPOSED

In 2018, ResTech Solutions analyzed 14.9 billion raw records. After the curation and verification process, validation confirmed around 3.6 billion identity records were new and authentic.

Even though the number of breaches was four times higher than in 2017, the number of real identity records in 2018 did not scale with the same magnitude. This reinforces the fact that the number of new identity records exposed continues to grow and previously exposed information increasingly re-circulates in underground communities.

3.6
BILLION
CURATED IDENTITY RECORDS IN 2018

5.4 OPEN DEVICES & DATABASES WIDELY EXPOSED IN 2018 5.4

As predicted in 2017, 2018 was a big year for open device exposure. Exactis and Apollo alone exposed 490 million records. Moving forward, as more companies monitor for leaks, ResTech Solutions anticipates open device incidents to be less of a concern in 2019 while still representing an easy target for hackers using automated crawlers.

13,931

NEW OPEN DEVICES SERVERS

18.952 GB

TOTAL STORAGE

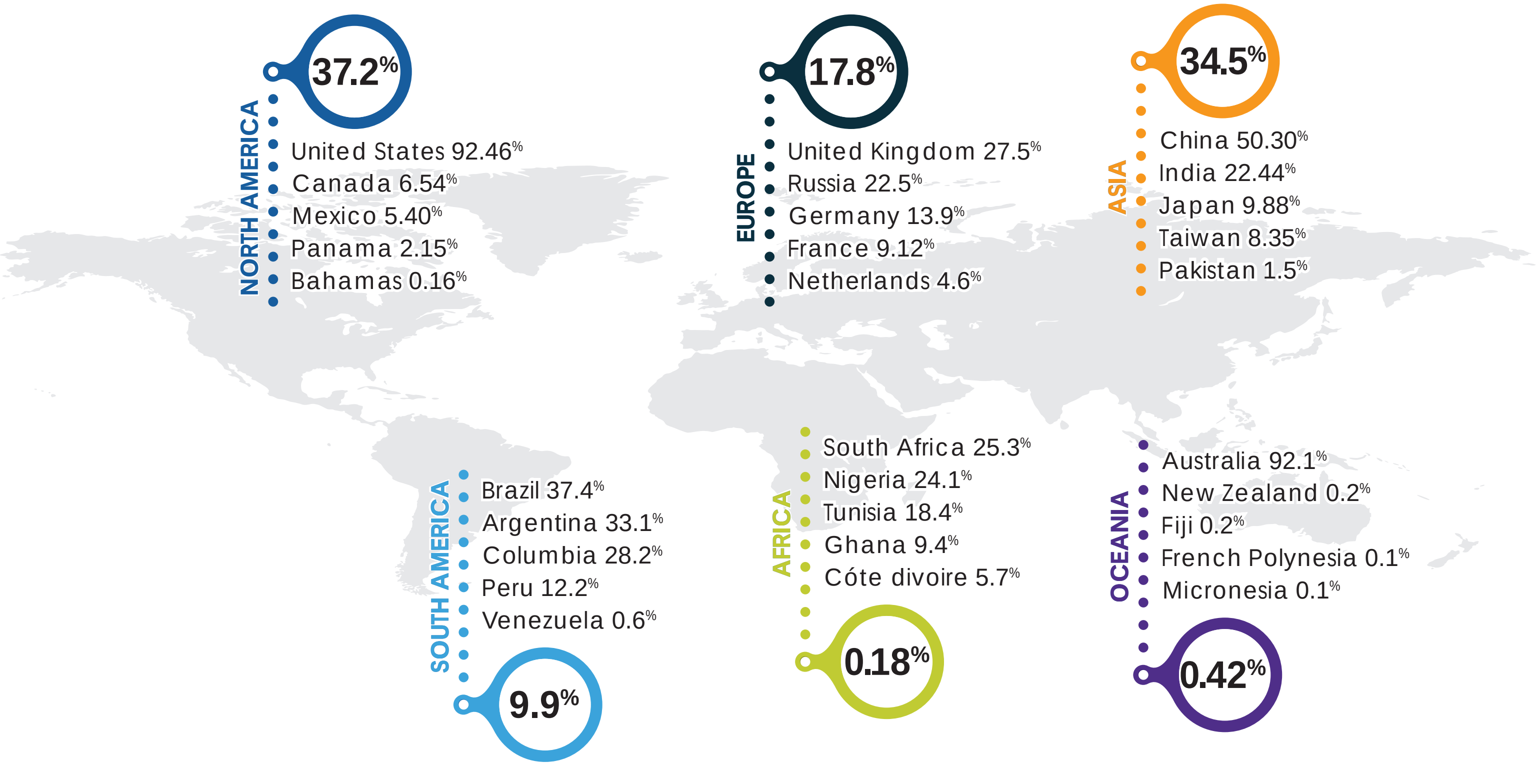
9,476 M

TOTAL RECORDS

(Assuming an average of 500M Records per TB exposed)

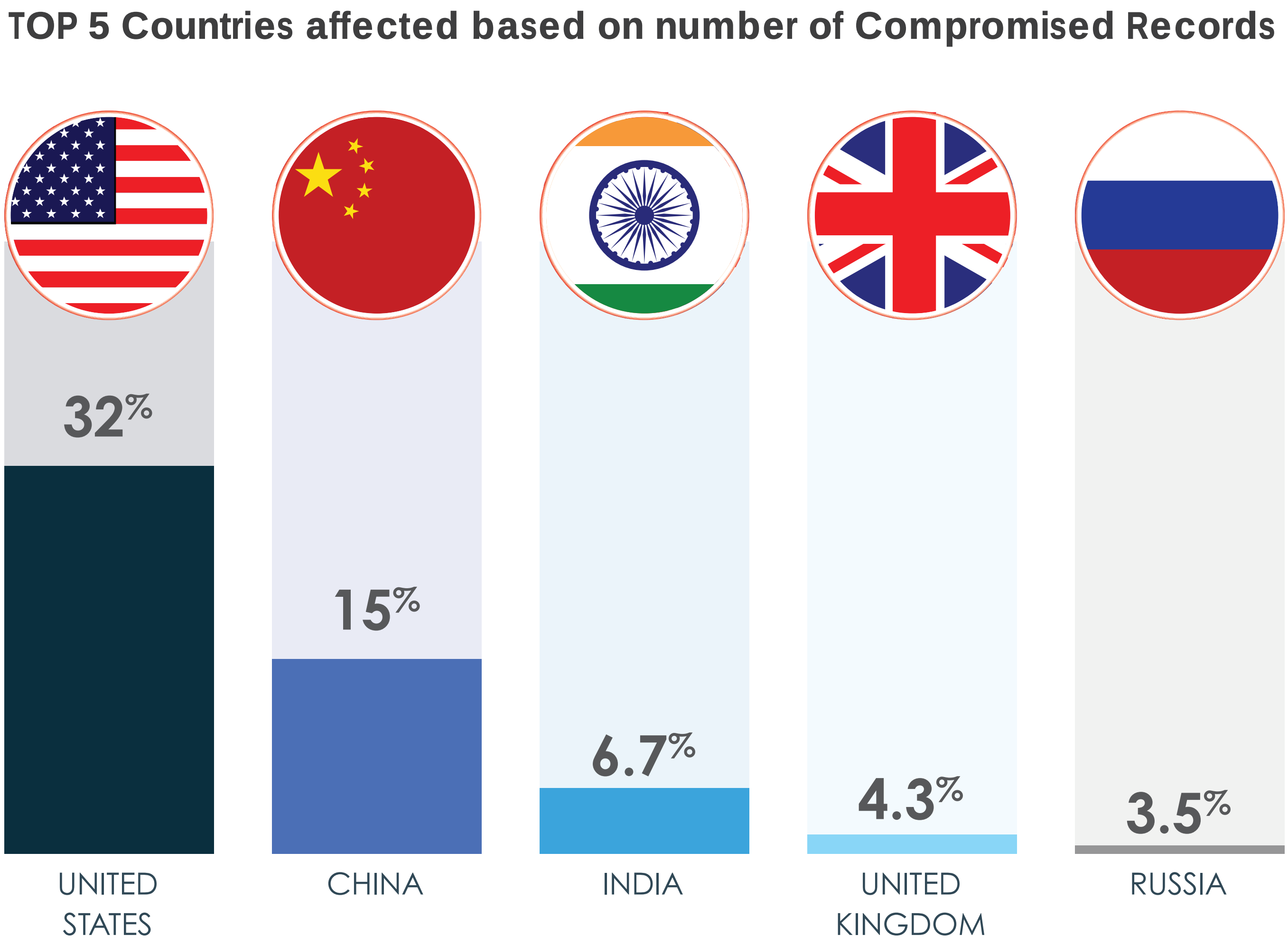
5.5 GEOGRAPHIC DISTRIBUTION OF BREACHES

The following map represents the total number of curated breaches detected in 2018. The percentage of breaches affecting each continent and top five countries are included. Although the number of breaches in the US are lower compared to other countries, the sheer volume of identity records per company or organization is typically much larger and a more valuable target for cyber criminals. Compared to 2017, we saw breach exposure growth in China, Russia, Vietnam, Japan, and Brazil.



5.6 TOP 5 COUNTRIES AFFECTED BASED ON NUMBER OF RECORDS EXPOSED IN 2018

Facing the largest number of attacks, exposed identities in the United States represented **32%** of all curated records detected in breaches in 2018. The top five countries account for more than **61.5%** of all identities compromised.



5.7 CURATED BREACHES BY INDUSTRY

The infographic below represents the distribution of real breaches relating to the industries we validated and inserted in our ResTech Solutions **IDLake™** in 2018.

27.5%	FORUMS & REFERRALS
12.2%	GOVERNMENT AGENCIES
11.8%	GAMING & GAMBLING
11.7%	E-COMMERCE
9.2%	EDUCATION & ACADEMIA
6.4%	NEWS & SPECIAL INTERESTS
4.7%	TRAVEL
3.3%	INFRASTRUCTURE
2.8%	SERVICES
2.7%	BANKING & FINANCE
2.1%	MEDIA ENTERTAINMENT
2.0%	HEALTHCARE
1.9%	ADULT
1.0%	SOCIAL MEDIA & DATING
0.7%	HACKING
0.2%	CRYPTO CURRENCY

Notable industry comparisons from 2017:

Government Agencies was the largest growing exposed sector in 2018, increasing **291%** from 2017, as citizen data interest grew significantly in 2018.

Forums and Referral sites were the highest category breached in 2018, hence its separation out from last year's category "professional, business tools and services." In 2017, new hacking tools were made available that automatically have exposed vulnerabilities in forums. In 2018, hackers were able to automatically use more advanced versions of these tools to exploit security weaknesses at scale.

Crypto-currency has been added as a new category after the first cryptocurrency sites were breached last year.

5.8 IDENTITY EXPOSURE BY TYPE

This graphic lists the type of exposed personal information, or attributes, that we find. Each breach typically contains only a small subset of attributes. Every data point is valuable to cyber criminals, and the more data they collect on an individual, the more valuable each set becomes.

PERSONAL DATA ATTRIBUTES

BANK INFORMATION
- Income Tax Number
- Bank Account Number
- IBAN
- Bank/Credit Card Number

IDENTIFIABLE INFORMATION
- Passport Number
- Drivers License
- Social Security Number
- National Id Number

MEDICAL INFORMATION
- Medical Insurance Provider
- Medical Insurance Number
- Insurance Account Number
- Insurance Provider

BUSINESS INFORMATION
- Company
- Domain Brand

PERSONAL INFORMATION
- Name
- Username
- Password
- Surname
- Phone Number
- Email
- Date of Birth
- Home Address
- Mother's Maiden Name

SIGNIFICANT NUMBER CONTAINED EMAILS AND PASSWORDS:

77%

Emails & Passwords Found

40%

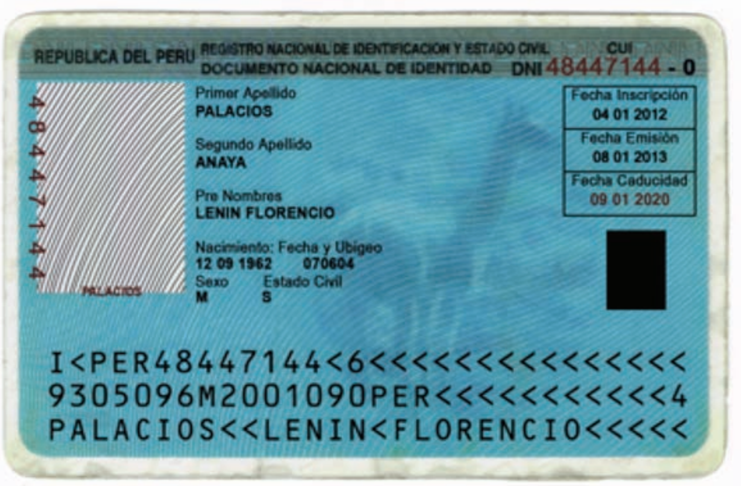
PII Attributes Discovered

6. EXAMPLES OF EXPOSED INFORMATION

FAKE IDENTITY KITS

A file with 21 million identities from Peruvian citizens was packaged with an Adobe Photoshop (.psd) file design template to create fake IDs. The file size totalled 1.6GB with the following exposed fields: National ID numbers, dates of birth, first names, last names, addresses and zip codes.

The package was organized by age and popular names so as to aid in making identity theft easier.



REPUBLICA DEL PERU REGISTRO NACIONAL DE IDENTIFICACION Y ESTADO CIVIL
DOCUMENTO NACIONAL DE IDENTIDAD CUI DNI 48447144 - 0

48447144

Primer Apellido
PALACIOS

Segundo Apellido
ANAYA

Pre Nombres
LENIN FLORENCIO

Nacimiento: Fecha y Ubigeo
12 09 1962 070604

Sexo M
Estado Civil S

PALACIOS

Fecha Inscripción
04 01 2012

Fecha Emisión
08 01 2013

Fecha Caducidad
09 01 2020

[redacted]

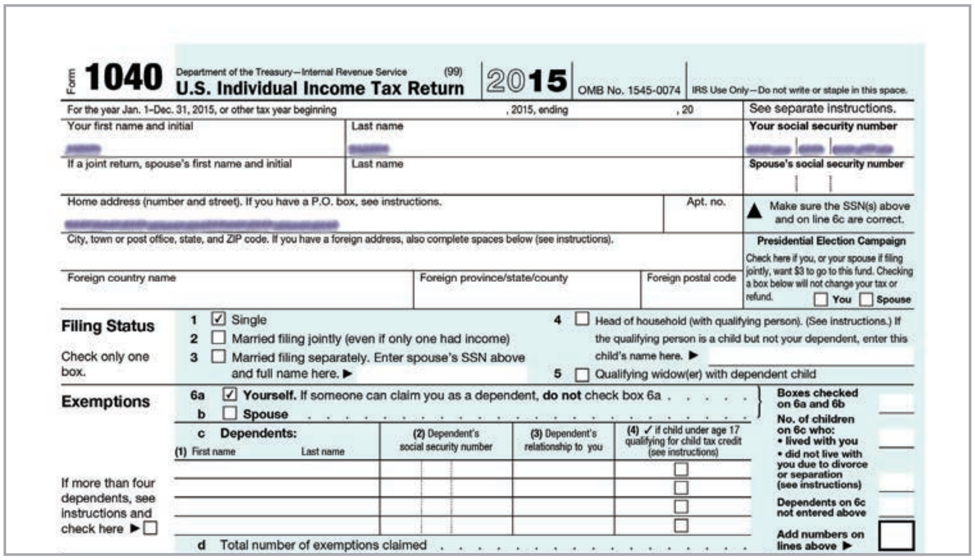
```
I<PER48447144<6<<<<<<<<<<<<<<<
9305096M2001090PER<<<<<<<<<<<4
PALACIOS<<LENIN<FLORENCIO<<<<<
```

.psd File - Peru Citizen ID Template

TAX DATA FOR SALE

This is an example of tax data for sale in underground marketplaces.

Tax data is sold with star ratings on the vendor, and includes the cost, shipping information, and other seller details just like any legal eCommerce site.



Form **1040** Department of the Treasury—Internal Revenue Service (99) **U.S. Individual Income Tax Return** **2015** OMB No. 1545-0074 IRS Use Only—Do not write or staple in this space.

For the year Jan. 1–Dec. 31, 2015, or other tax year beginning , 2015, ending , 20 See separate instructions.

Your first name and initial [redacted] Last name [redacted] **Your social security number** [redacted]

If a joint return, spouse's first name and initial Last name **Spouse's social security number**

Home address (number and street). If you have a P.O. box, see instructions. [redacted] Apt. no. ▲ Make sure the SSN(s) above and on line 6c are correct.

City, town or post office, state, and ZIP code. If you have a foreign address, also complete spaces below (see instructions).

Presidential Election Campaign Check here if you, or your spouse if filing jointly, want $3 to go to this fund. Checking a box below will not change your tax or refund. □ You □ Spouse

Foreign country name Foreign province/state/county Foreign postal code

Filing Status

Check only one box.

1 ☑ Single
2 □ Married filing jointly (even if only one had income)
3 □ Married filing separately. Enter spouse's SSN above and full name here. ▶
4 □ Head of household (with qualifying person). (See instructions.) If the qualifying person is a child but not your dependent, enter this child's name here. ▶
5 □ Qualifying widow(er) with dependent child

Exemptions

6a ☑ **Yourself.** If someone can claim you as a dependent, **do not** check box 6a . . . . . .
b □ **Spouse** . . . .

Boxes checked on 6a and 6b

c **Dependents:** (1) First name Last name	(2) Dependent's social security number	(3) Dependent's relationship to you	(4) ✓ if child under age 17 qualifying for child tax credit (see instructions)
			□
			□
			□
			□

If more than four dependents, see instructions and check here ▶ □

No. of children on 6c who:
• lived with you
• did not live with you due to divorce or separation (see instructions)
Dependents on 6c not entered above

d Total number of exemptions claimed . . . .

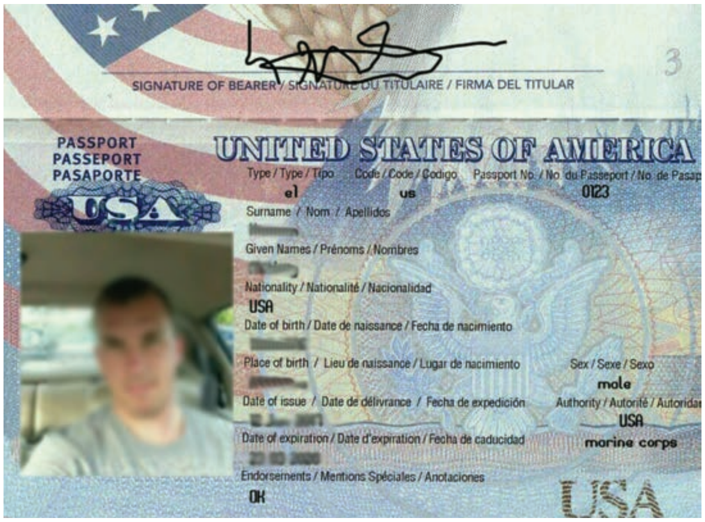
Add numbers on lines above ▶

TAX DATA (1040-W2) 2015-2016 (TAX RETURN FILES)

Vendor	[redacted] (4.82★) (ⓐ 453/6/17)
Price	€45.912
Ships tp	Worlwide
Ships from	Worlwide
Escrow	Yes

PASSPORTS

Here are just some examples of passports exposed in underground marketplaces.



SIGNATURE OF BEARER / SIGNATURE DU TITULAIRE / FIRMA DEL TITULAR

3

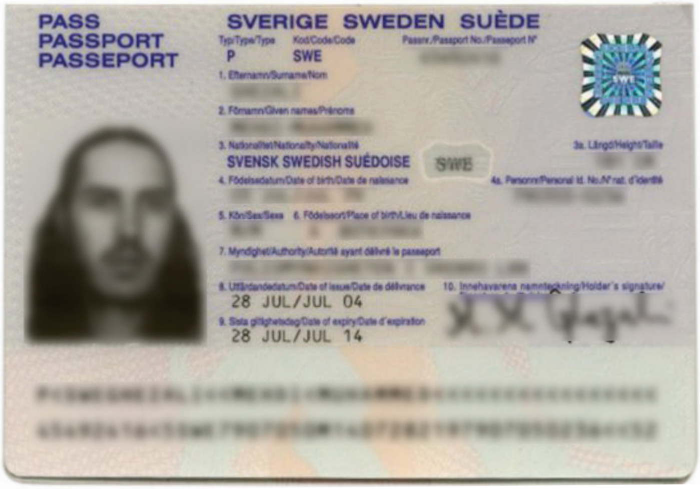
PASSPORT
PASSEPORT
PASAPORTE

USA

UNITED STATES OF AMERICA

Type / Type / Tipo: el
Code / Code / Codigo: us
Passport No. / No. du Passeport / No. de Pasap: 0123
Surname / Nom / Apellidos: [redacted]
Given Names / Prénoms / Nombres: [redacted]
Nationality / Nationalité / Nacionalidad: USA
Date of birth / Date de naissance / Fecha de nacimiento: [redacted]
Place of birth / Lieu de naissance / Lugar de nacimiento: [redacted]
Sex / Sexe / Sexo: male
Date of issue / Date de délivrance / Fecha de expedición: [redacted]
Authority / Autorité / Autoridad: USA marine corps
Date of expiration / Date d'expiration / Fecha de caducidad: [redacted]
Endorsements / Mentions Spéciales / Anotaciones: OK

USA



PASS
PASSPORT
PASSEPORT

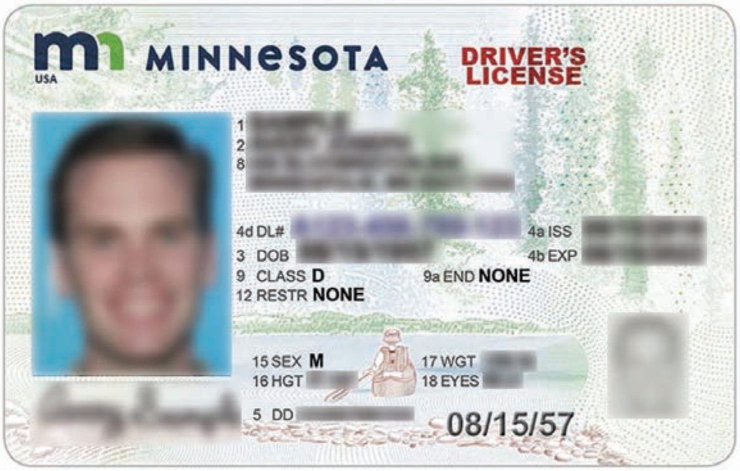
SVERIGE SWEDEN SUÈDE

Typ/Type/Type: P
Kod/Code/Code: SWE
Passnr./Passport No./Passeport N°: [redacted]
1. Efternamn/Surname/Nom: [redacted]
2. Förnamn/Given names/Prénoms: [redacted]
3. Nationalitet/Nationality/Nationalité: SVENSK SWEDISH SUÉDOISE
SWE
3a. Längd/Height/Taille: [redacted]
4. Födelsedatum/Date of birth/Date de naissance: [redacted]
4a. Personnr/Personal Id. No./N° nat. d'identité: [redacted]
5. Kön/Sex/Sexe: [redacted]
6. Födelseort/Place of birth/Lieu de naissance: [redacted]
7. Myndighet/Authority/Autorité ayant délivré le passeport: [redacted]
8. Utfärdandedatum/Date of issue/Date de délivrance: 28 JUL/JUL 04
9. Sista giltighetsdag/Date of expiry/Date d'expiration: 28 JUL/JUL 14
10. Innehavarens namnteckning/Holder's signature/

[redacted]

DRIVER'S LICENSES

Driver's licenses are also circulating for sale in the deep and dark web.



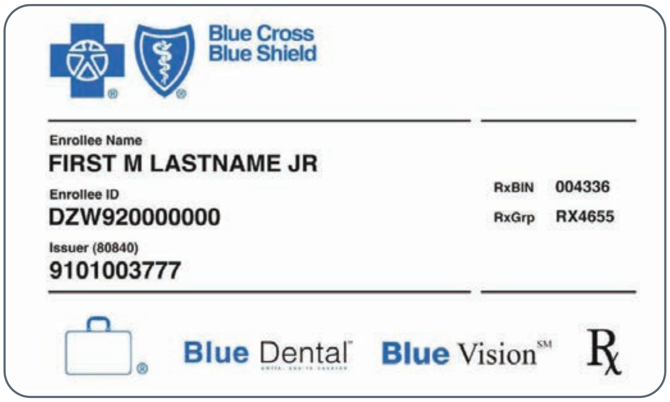
mn USA MINNESOTA DRIVER'S LICENSE

1 [redacted]
2
8

4d DL# [redacted]
4a ISS [redacted]
3 DOB [redacted]
4b EXP [redacted]
9 CLASS D
9a END NONE
12 RESTR NONE
15 SEX M
16 HGT [redacted]
17 WGT [redacted]
18 EYES [redacted]
5 DD [redacted]
08/15/57

INSURANCE CARDS

Forged Health Insurance cards are for sale for $72.8, and can be shipped from the United States anywhere in the world.



Blue Cross Blue Shield

Enrollee Name
FIRST M LASTNAME JR

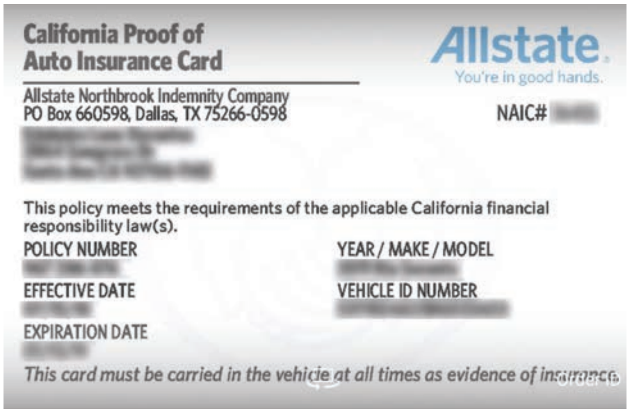
Enrollee ID
DZW920000000

Issuer (80840)
9101003777

RxBIN 004336
RxGrp RX4655

Blue Dental Blue Vision℠ ℞

Auto Insurance Cards for sale, complete with product descriptions.



California Proof of Auto Insurance Card

Allstate. You're in good hands.

Allstate Northbrook Indemnity Company
PO Box 660598, Dallas, TX 75266-0598

NAIC# [redacted]

[redacted]

This policy meets the requirements of the applicable California financial responsibility law(s).

POLICY NUMBER
[redacted]

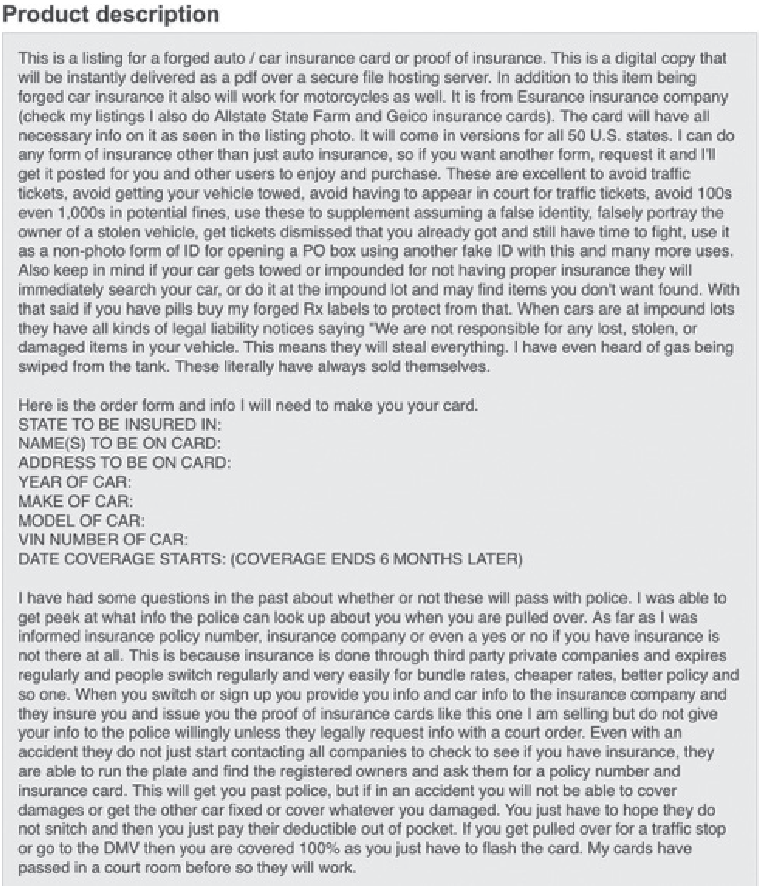
EFFECTIVE DATE
[redacted]

EXPIRATION DATE
[redacted]

YEAR / MAKE / MODEL
[redacted]

VEHICLE ID NUMBER
[redacted]

This card must be carried in the vehicle at all times as evidence of insurance.



Product description

This is a listing for a forged auto / car insurance card or proof of insurance. This is a digital copy that will be instantly delivered as a pdf over a secure file hosting server. In addition to this item being forged car insurance it also will work for motorcycles as well. It is from Esurance insurance company (check my listings I also do Allstate State Farm and Geico insurance cards). The card will have all necessary info on it as seen in the listing photo. It will come in versions for all 50 U.S. states. I can do any form of insurance other than just auto insurance, so if you want another form, request it and I'll get it posted for you and other users to enjoy and purchase. These are excellent to avoid traffic tickets, avoid getting your vehicle towed, avoid having to appear in court for traffic tickets, avoid 100s even 1,000s in potential fines, use these to supplement assuming a false identity, falsely portray the owner of a stolen vehicle, get tickets dismissed that you already got and still have time to fight, use it as a non-photo form of ID for opening a PO box using another fake ID with this and many more uses. Also keep in mind if your car gets towed or impounded for not having proper insurance they will immediately search your car, or do it at the impound lot and may find items you don't want found. With that said if you have pills buy my forged Rx labels to protect from that. When cars are at impound lots they have all kinds of legal liability notices saying "We are not responsible for any lost, stolen, or damaged items in your vehicle. This means they will steal everything. I have even heard of gas being swiped from the tank. These literally have always sold themselves.

Here is the order form and info I will need to make you your card.
STATE TO BE INSURED IN:
NAME(S) TO BE ON CARD:
ADDRESS TO BE ON CARD:
YEAR OF CAR:
MAKE OF CAR:
MODEL OF CAR:
VIN NUMBER OF CAR:
DATE COVERAGE STARTS: (COVERAGE ENDS 6 MONTHS LATER)

I have had some questions in the past about whether or not these will pass with police. I was able to get peek at what info the police can look up about you when you are pulled over. As far as I was informed insurance policy number, insurance company or even a yes or no if you have insurance is not there at all. This is because insurance is done through third party private companies and expires regularly and people switch regularly and very easily for bundle rates, cheaper rates, better policy and so one. When you switch or sign up you provide you info and car info to the insurance company and they insure you and issue you the proof of insurance cards like this one I am selling but do not give your info to the police willingly unless they legally request info with a court order. Even with an accident they do not just start contacting all companies to check to see if you have insurance, they are able to run the plate and find the registered owners and ask them for a policy number and insurance card. This will get you past police, but if in an accident you will not be able to cover damages or get the other car fixed or cover whatever you damaged. You just have to hope they do not snitch and then you just pay their deductible out of pocket. If you get pulled over for a traffic stop or go to the DMV then you are covered 100% as you just have to flash the card. My cards have passed in a court room before so they will work.

7. DEFINITIONS

IDENTITY RECORDS DEFINED

Identity Record

An identity record is one or more pieces of information – identity attributes – containing personally identifiable information (PII) such as name, username, password, address, phone etc., linked to a single individual.

Raw Identity Record

A raw identity record is a record found in the wild which has not yet been curated and validated. During the curation and validation process, the record could be found to be an exact or partial duplicate of information in another data dump, or the data could be determined to be fake.

Curated Identity Record

A curated identity record is an identity record that has been validated and found to be both real and authentic (not fake) and original (not a duplicate, exposed or seen in another data dump or breach corpus before).

WHAT IS AN INCIDENT?

ResTech Solutions defines an **incident** as an event in which a company has had a vulnerability exposed, but where there has not been any confirmation that the data has been stolen.

WHAT IS A DATA BREACH?

ResTech Solutions defines a **data breach** as a confirmed incident where credentials, personal, medical, financial or other records with sensitive data have been accessed or disclosed due to being hacked or leaked, either deliberately or by accident.

WHAT IS AN 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 configurations or misconfigurations of anonymous FTP servers and cloud-based databases (e.g. MongoDB) to lost laptops, tablets or mobile phones containing or providing access to sensitive information.

8. ABOUT RESTECH SOLUTIONS

ResTech Solutions is an identity intelligence company on a mission to empower intelligence analysts, security researchers, and criminal investigators with capabilities to discover, uncover, and disrupt adversaries and prevent billions of dollars in fraud losses, account takeover, and cyber espionage.

The ResTech Solutions Cyber Security Platform archives more than 14 billion identity records collected from open source data breaches and leaks on the surface, social, and deep and dark web. When ResTech Solutions researchers find breaches, they reach out directly to the security representatives of a company in any way possible and work with them to help close their leaking devices or recommend next steps to breach disclosures. The ResTech Solutions team uses an extensive verification process to determine the breach source, and whether the information in a data dump is real and not a duplicate copy of an earlier package.

The ResTech Solutions Cyber Security Platorm powers the ResTech Solutions **PIISecured** solution used by some of the largest identity theft protection service providers, security vendors, and enterprises, to alert millions of consumers of exposed personal information. We only report breaches when confidence levels are high, and each exposure alert sent to a consumer or company includes information on the breach as well as a risk rating of the potential impact of the exposure so that appropriate actions may be taken.

The ResTech Solutions Cyber Security Platorm also powers ResTech Solutions **IDHunt™**, a pioneering identity intelligence and attribution analysis solution used by fraud investigation units, anti-money laundering and financial crime intelligence units, and advanced security operations centers. ResTech Solutuions **IDHunt™** is a unified investigation platform supporting multiple objectives, missions, and units. The platform supports the full intelligence lifecycle – open source data collection, fusion with internal sources and 3rd party data, entity extraction and enrichment, dynamic taxonomies and data classification, automatic linking, tracking, alerting, collaboration, identity attribution analysis, and report generation.

This breach report is based on our findings, what we have seen, and what we have been able to analyze with respect to breaches and leaks in 2018. It is by no means a complete picture of the identity threat landscape, simply our view and contribution to helping people and their companies defend themselves.

ResTech Solutions Headquarters

8715 Meadowcroft Dr. #102
Houston, TX 77063

ILLUMINATING THE DARK WEB℠

www.restech.solutions