GDPArrrrr: Using Privacy Laws to Steal Identities

James Pavur

DPhil Student & Rhodes Scholar at Oxford University

Cybersecurity Center for Doctoral Training

Cyber(Law) Kill Chain

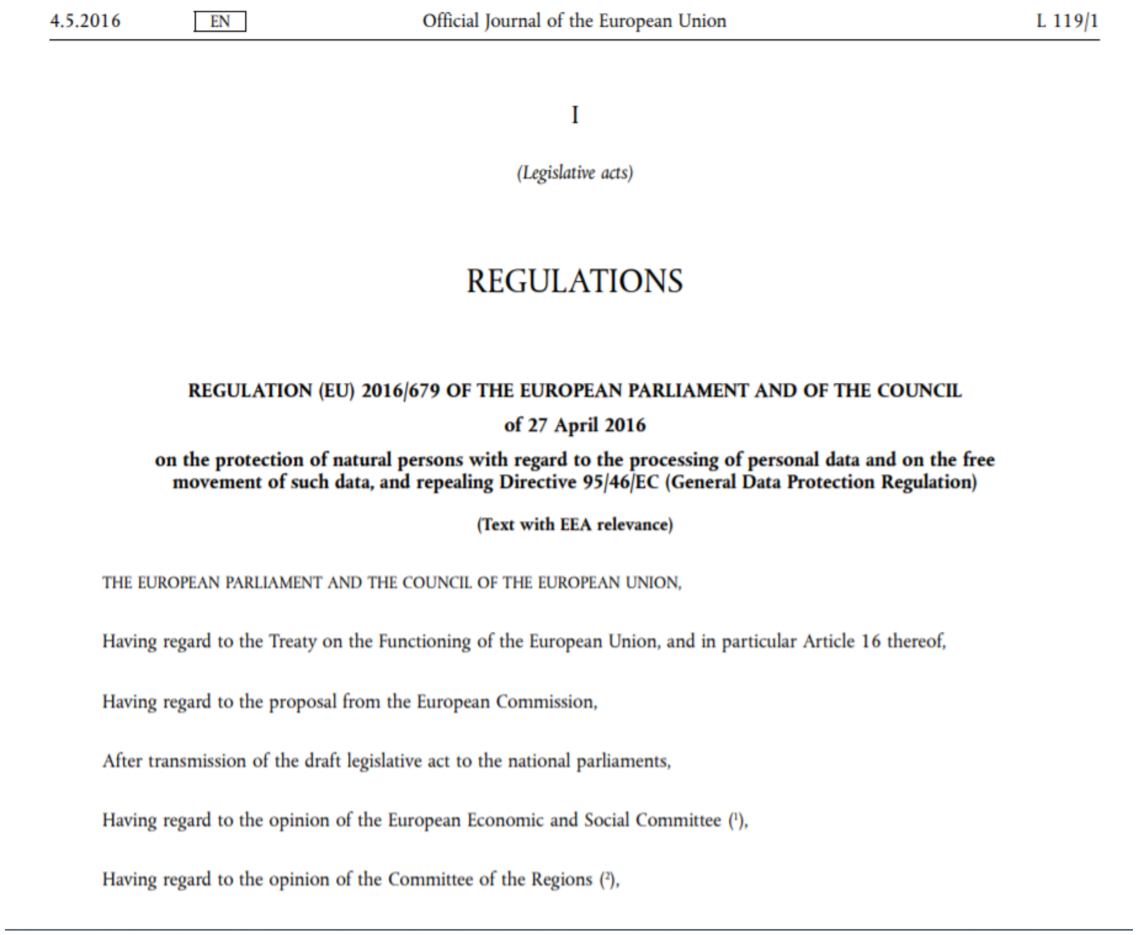
RECONNAISSANCE

WEAPONIZATION

DELIVERY

EXPLOITATION

EXFILTRATION



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the Committee of the Regions [2],

RECONNAISSANCE

Exploitable Properties of GDPR

Fear

Huge fines and reputational costs

Pressure

Proscribed time schedules and deadlines

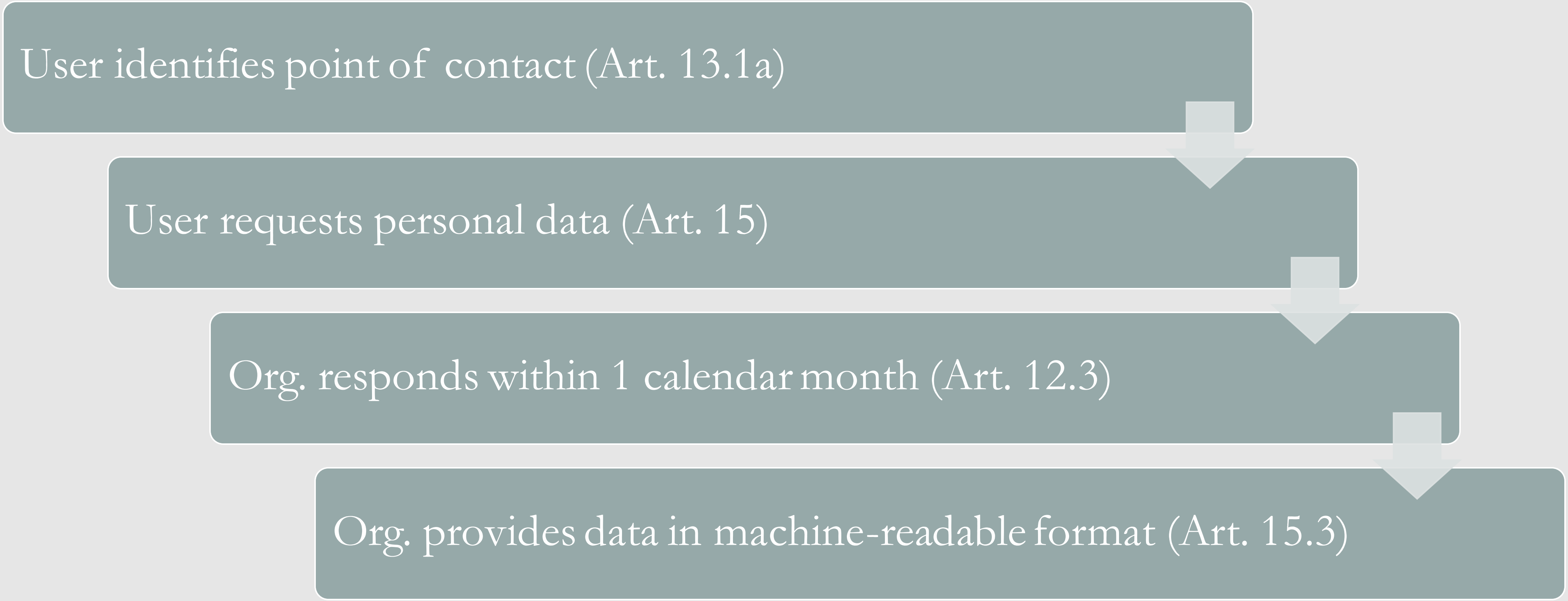
Ambiguity

Flexible terminology to ensure broad applicability

Humanity

Process complexity keeps humans in the loop

Target: Right of Access (Ch. III, Sec. 2)



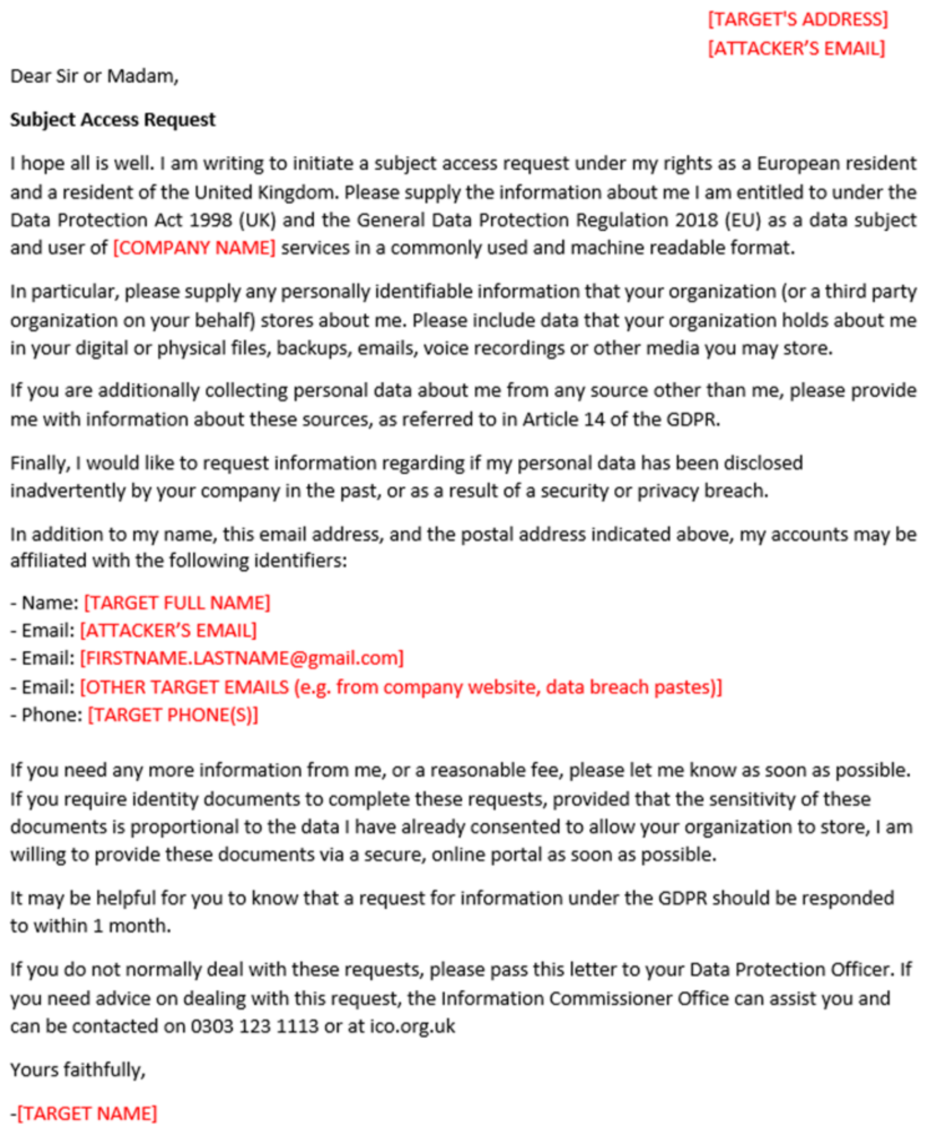
User identifies point of contact (Art. 13.1a)

User requests personal data (Art. 15)

Org. responds within 1 calendar month (Art. 12.3)

Org. provides data in machine-readable format (Art. 15.3)

WEAPONIZATION



[TARGET'S ADDRESS]
[ATTACKER'S EMAIL]

Dear Sir or Madam,

Subject Access Request

I hope all is well. I am writing to initiate a subject access request under my rights as a European resident and a resident of the United Kingdom. Please supply the information about me I am entitled to under the Data Protection Act 1998 (UK) and the General Data Protection Regulation 2018 (EU) as a data subject and user of [COMPANY NAME] services in a commonly used and machine readable format.

In particular, please supply any personally identifiable information that your organization (or a third party organization on your behalf) stores about me. Please include data that your organization holds about me in your digital or physical files, backups, emails, voice recordings or other media you may store.

If you are additionally collecting personal data about me from any source other than me, please provide me with information about these sources, as referred to in Article 14 of the GDPR.

Finally, I would like to request information regarding if my personal data has been disclosed inadvertently by your company in the past, or as a result of a security or privacy breach.

In addition to my name, this email address, and the postal address indicated above, my accounts may be affiliated with the following identifiers:

- Name: [TARGET FULL NAME]
- Email: [ATTACKER'S EMAIL]
- Email: [FIRSTNAME.LASTNAME@gmail.com]
- Email: [OTHER TARGET EMAILS (e.g. from company website, data breach pastes)]
- Phone: [TARGET PHONE(S)]

If you need any more information from me, or a reasonable fee, please let me know as soon as possible. If you require identity documents to complete these requests, provided that the sensitivity of these documents is proportional to the data I have already consented to allow your organization to store, I am willing to provide these documents via a secure, online portal as soon as possible.

It may be helpful for you to know that a request for information under the GDPR should be responded to within 1 month.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer. If you need advice on dealing with this request, the Information Commissioner Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

Yours faithfully,

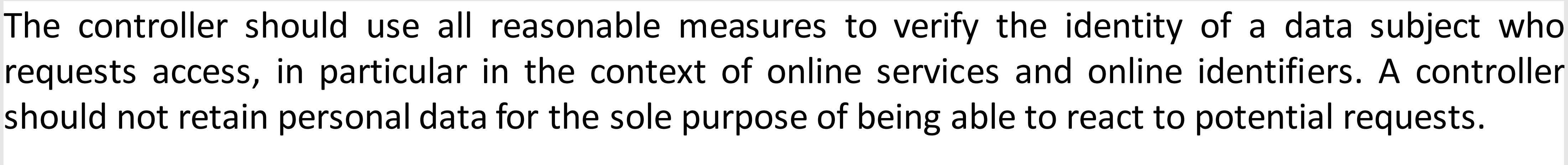
-[TARGET NAME]

Threat model (OSINT)

In addition to my name, this email address, and the postal address indicated above, my accounts may be affiliated with the following identifiers:

- *Name:* [TARGET FULL NAME]
- *Email:* [ATTACKER’S EMAIL]
- *Email:* [FIRSTNAME.LASTNAME@gmail.com]
- *Email:* [OTHER TARGET EMAILS (e.g. from company website, data breach pastes)]
- *Phone:* [TARGET PHONE(S)]

Problem: What if they ask for ID?



The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

- Recital 64 of GDPR

Problem: What if they ask for ID?

The controller should use all reasonable measures to ve the identity of a data subject who requests access, in particular in the context of online se es and online identifiers. A controller should not retain personal data for the sole purpose ng able to react to potential requests.

- Recital 64 of GDPR

Make “reasonable” workable

If you need any more information from me, or a reasonable fee, please let me know as soon as possible. If you require? identity documents to complete these requests, provided that the sensitivity of these documents is **proportional** *to the data I have already consented to allow your organization to store,* I am willing to provide these documents *via a secure, online portal as soon as possible.*

It may be helpful for you to know that a request for information under the GDPR should be responded to within 1 month.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer. If you need advice on dealing with this request, the Information Commissioner Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

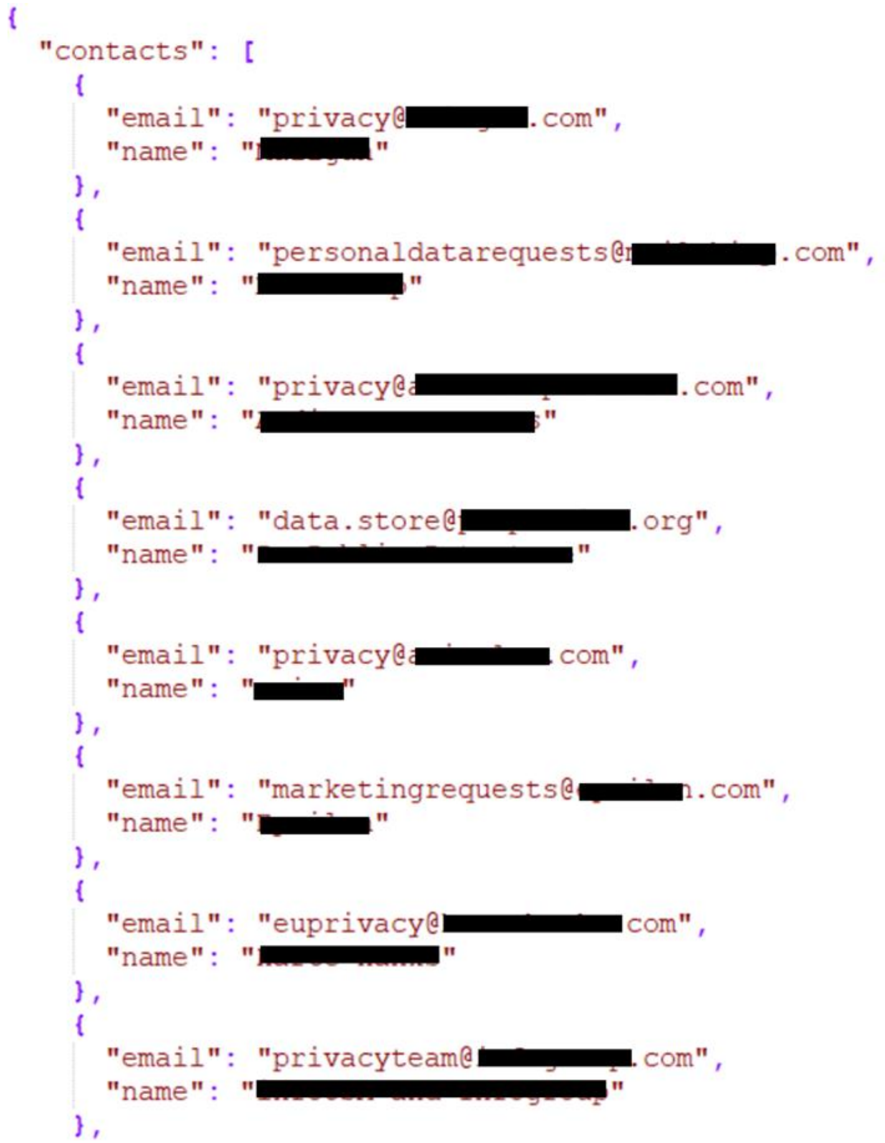
Dictate the terms of engagement

If you need any more information from me, or a reasonable fee, please let me know as soon as possible. If you require identity documents to complete these requests, provided that the sensitivity of these documents is proportional to the data I have already consented to allow your organization to store, I am willing to provide these documents via a secure, online portal *as soon as possible.* ? 😲

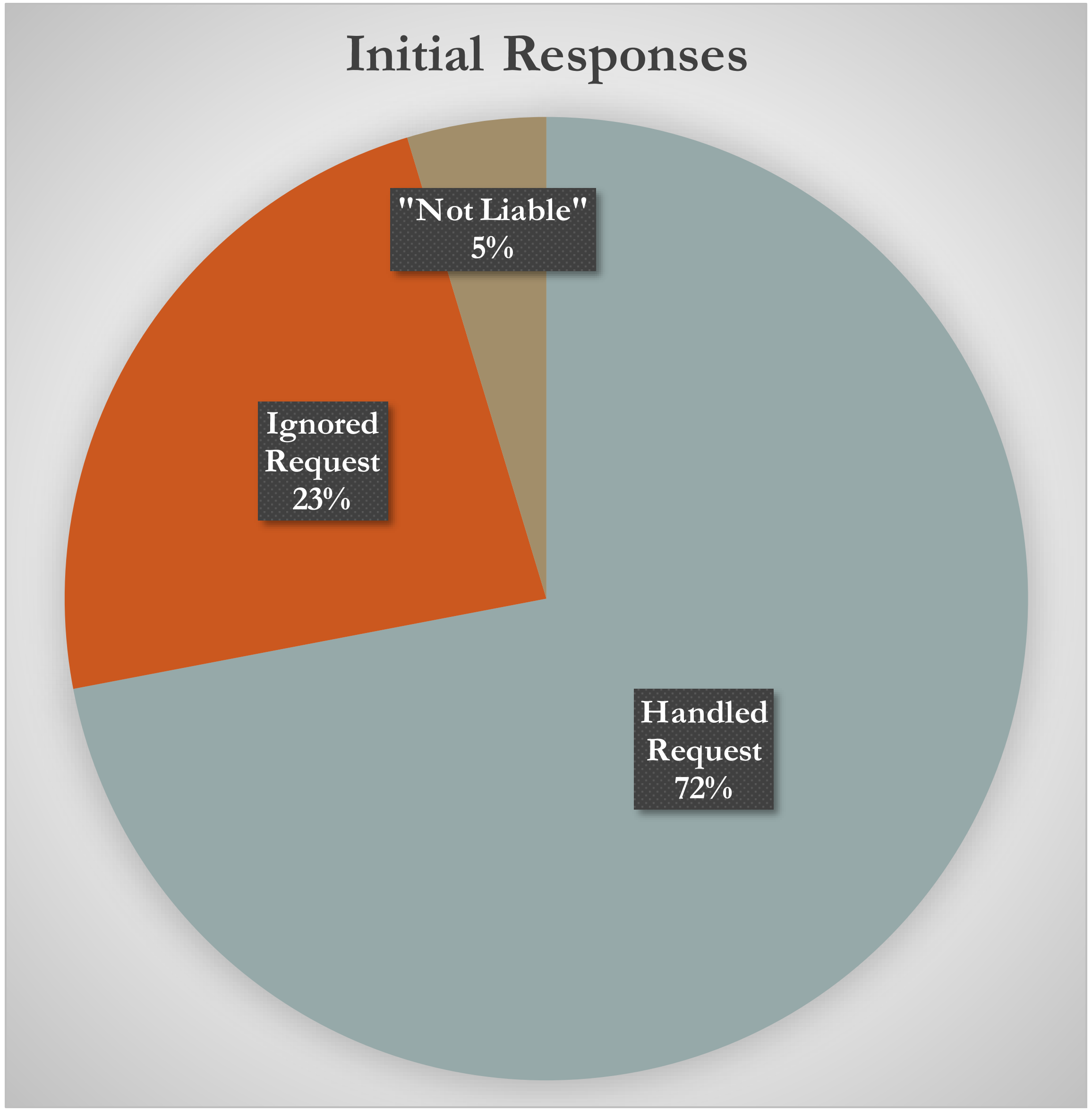
It may be helpful for you to know that a request for information under the GDPR should be responded to within 1 month.

If you do not normally deal with these requests, please pass this letter to your Data Protection Officer. If you need advice on dealing with this request, the Information Commissioner Office can assist you and can be contacted on 0303 123 1113 or at ico.org.uk

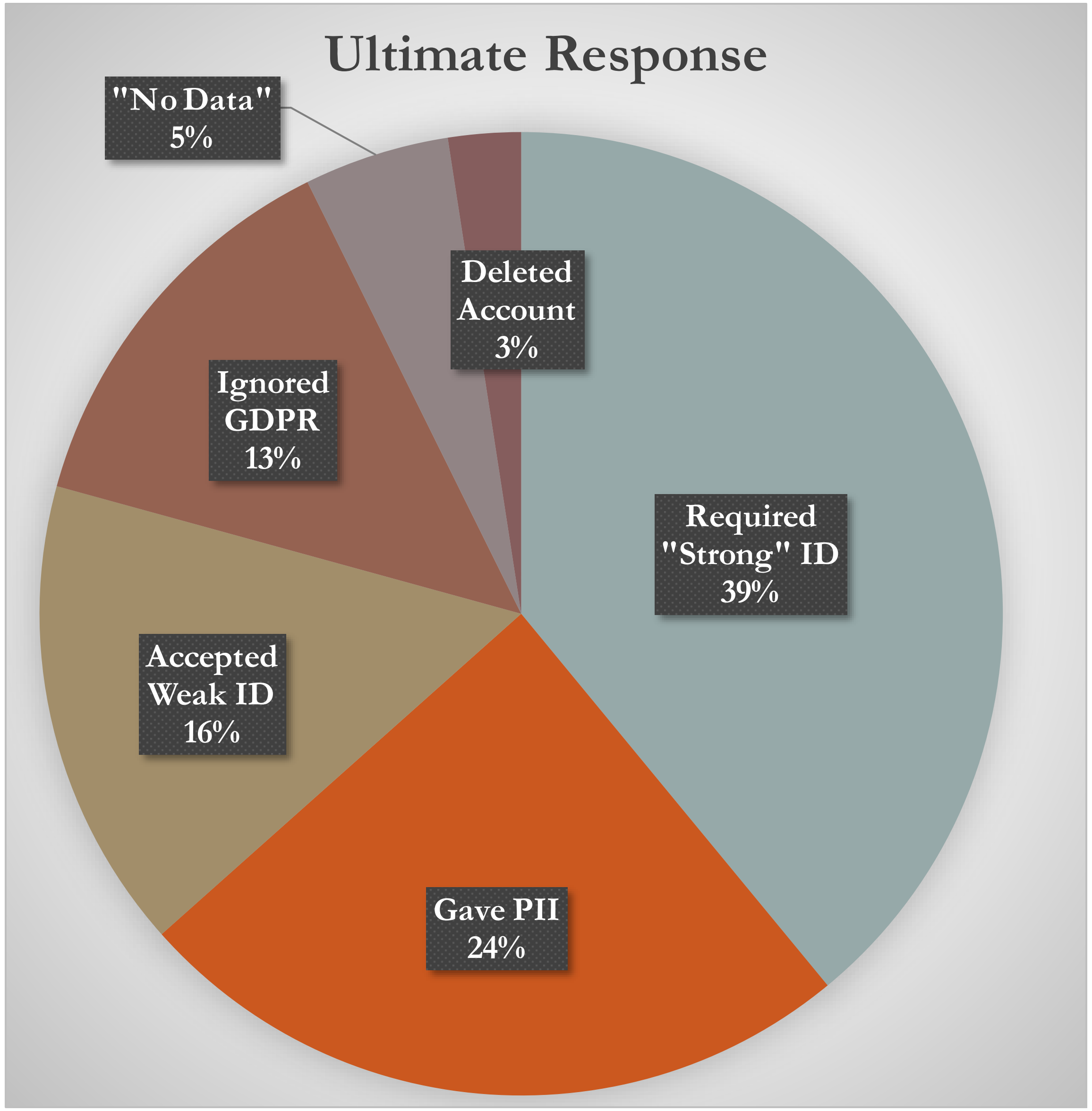
DELIVERY



```
{
  "contacts": [
    {
      "email": "privacy@[redacted].com",
      "name": "[redacted]"
    },
    {
      "email": "personaldatarequests@[redacted].com",
      "name": "[redacted]"
    },
    {
      "email": "privacy@[redacted].com",
      "name": "[redacted]"
    },
    {
      "email": "data.store@[redacted].org",
      "name": "[redacted]"
    },
    {
      "email": "privacy@[redacted]com",
      "name": "[redacted]"
    },
    {
      "email": "marketingrequests@[redacted].com",
      "name": "[redacted]"
    },
    {
      "email": "euprivacy@[redacted]com",
      "name": "[redacted]"
    },
    {
      "email": "privacyteam@[redacted].com",
      "name": "[redacted]"
    },
```

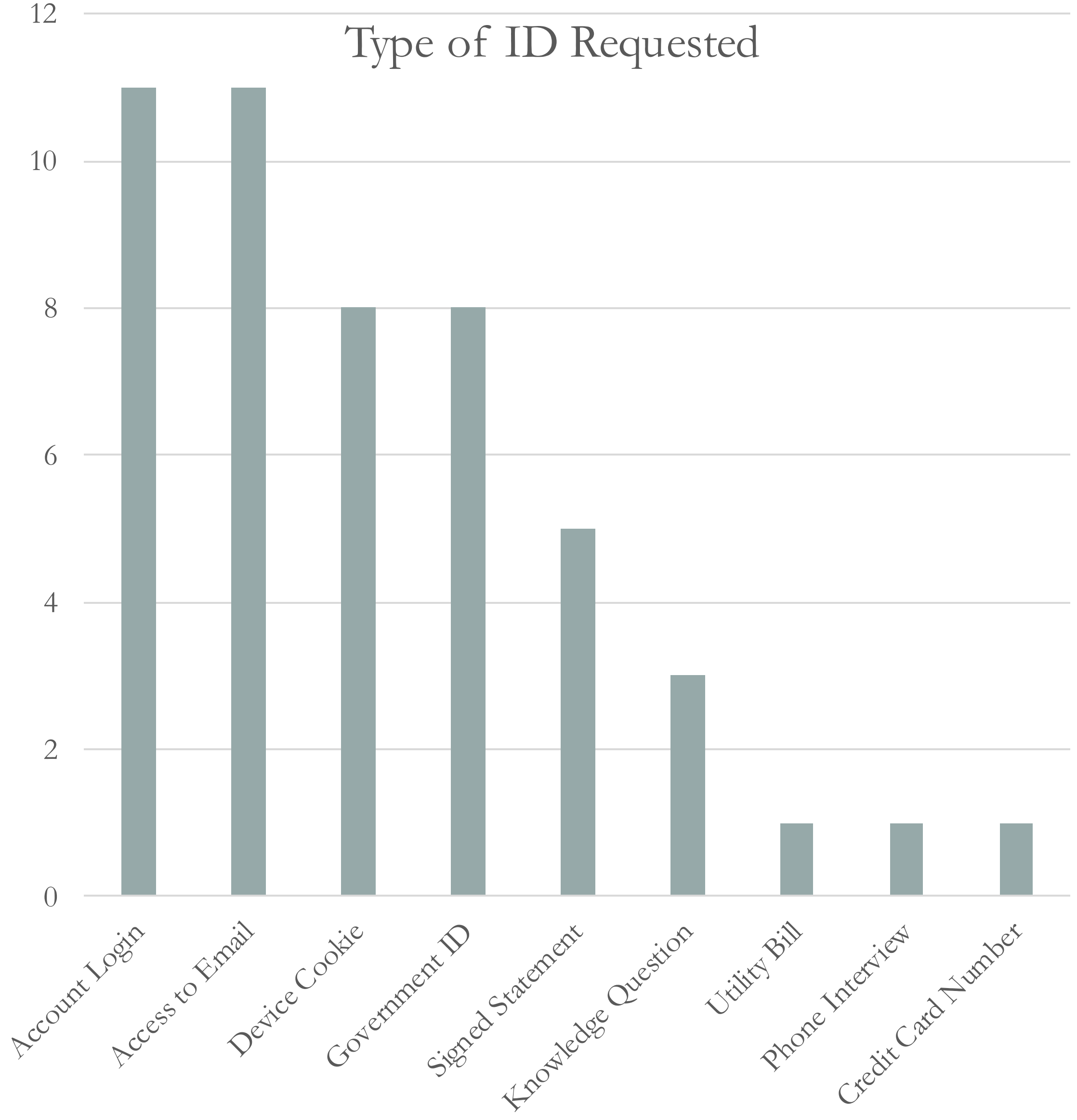


EXPLOITATION



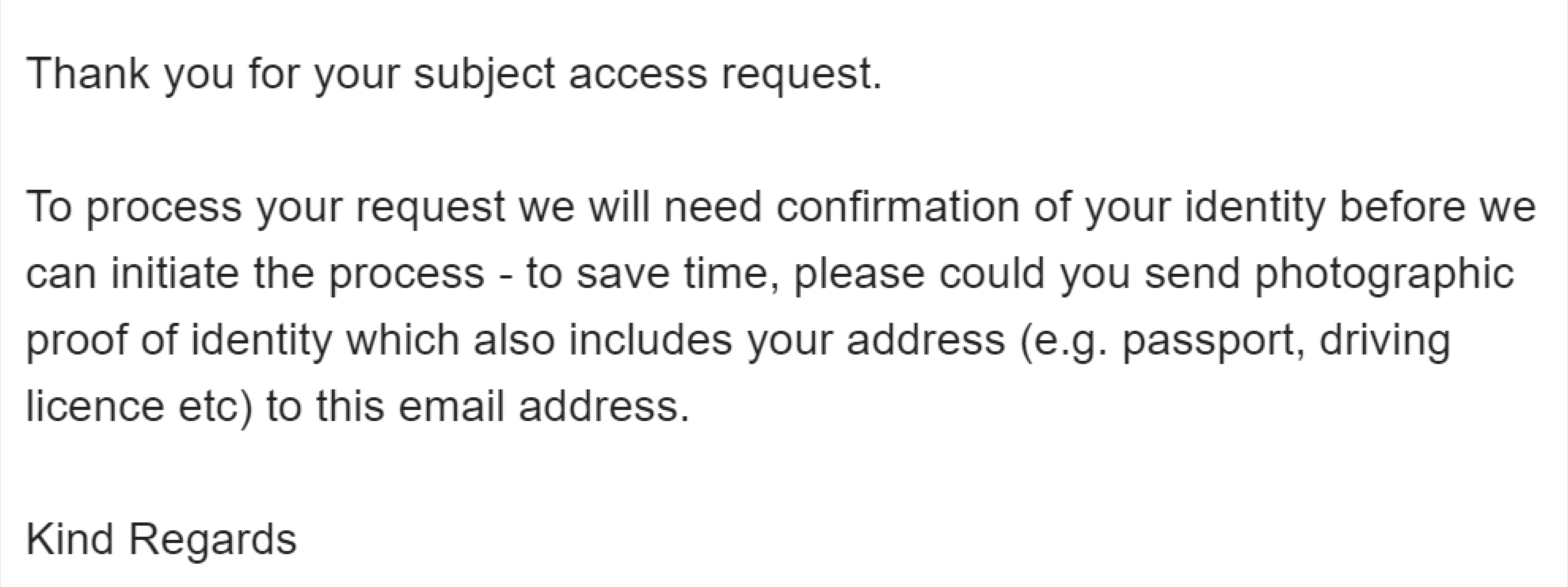
HIGH VARIATION IN ULTIMATE OUTCOMES

OF THE 83 ORGANIZATIONS WHICH HAD "VICTIM'S" PII….



NO CLEAR STANDARD FOR “REASONABLE” ID VERIFICATION

A Rejected Request?

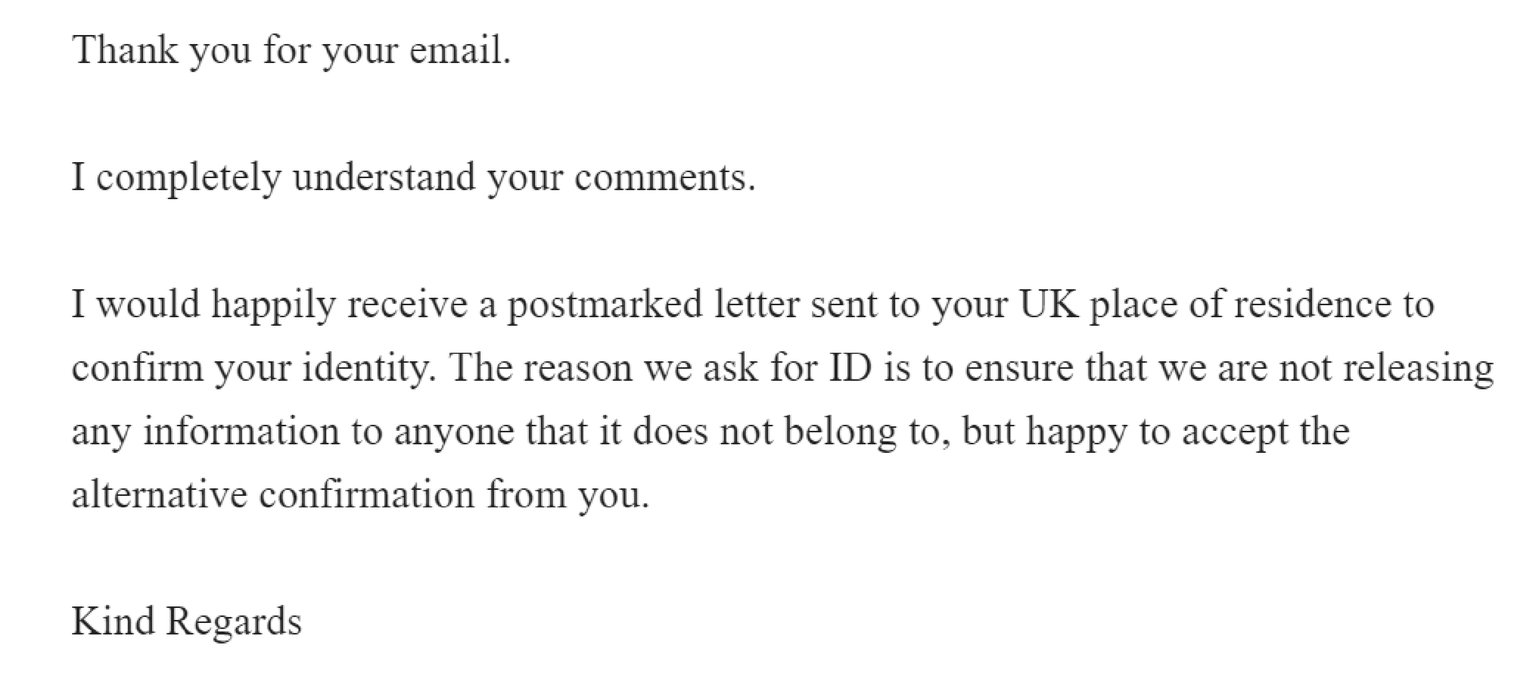


Thank you for your subject access request.

To process your request we will need confirmation of your identity before we can initiate the process - to save time, please could you send photographic proof of identity which also includes your address (e.g. passport, driving licence etc) to this email address.

Kind Regards

Never Give Up!



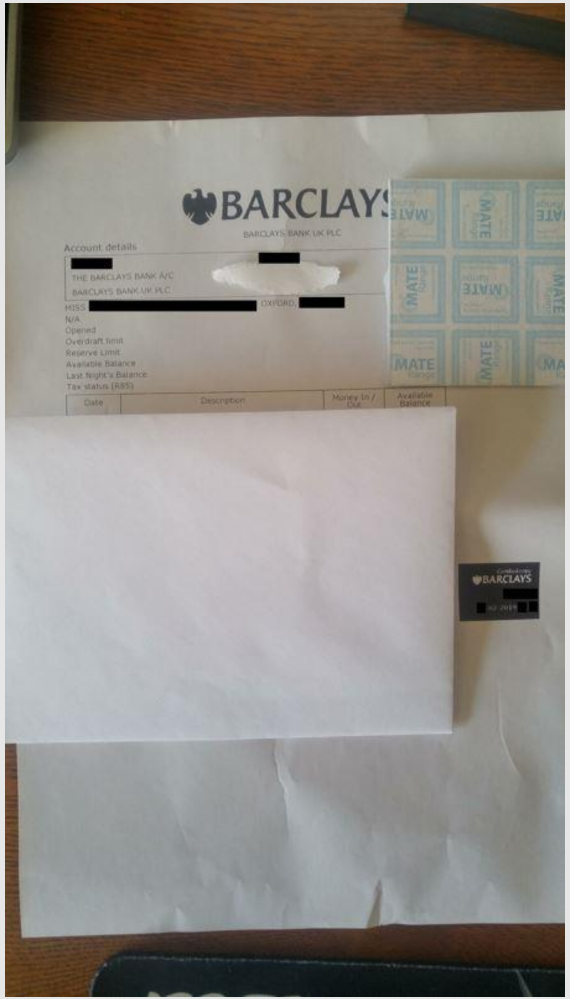
Thank you for your email.

I completely understand your comments.

I would happily receive a postmarked letter sent to your UK place of residence to confirm your identity. The reason we ask for ID is to ensure that we are not releasing any information to anyone that it does not belong to, but happy to accept the alternative confirmation from you.

Kind Regards

Never Give Up!



BARCLAYS

BARCLAYS BANK UK PLC

Account details

[redacted] [redacted]

THE BARCLAYS BANK A/C

BARCLAYS BANK UK PLC

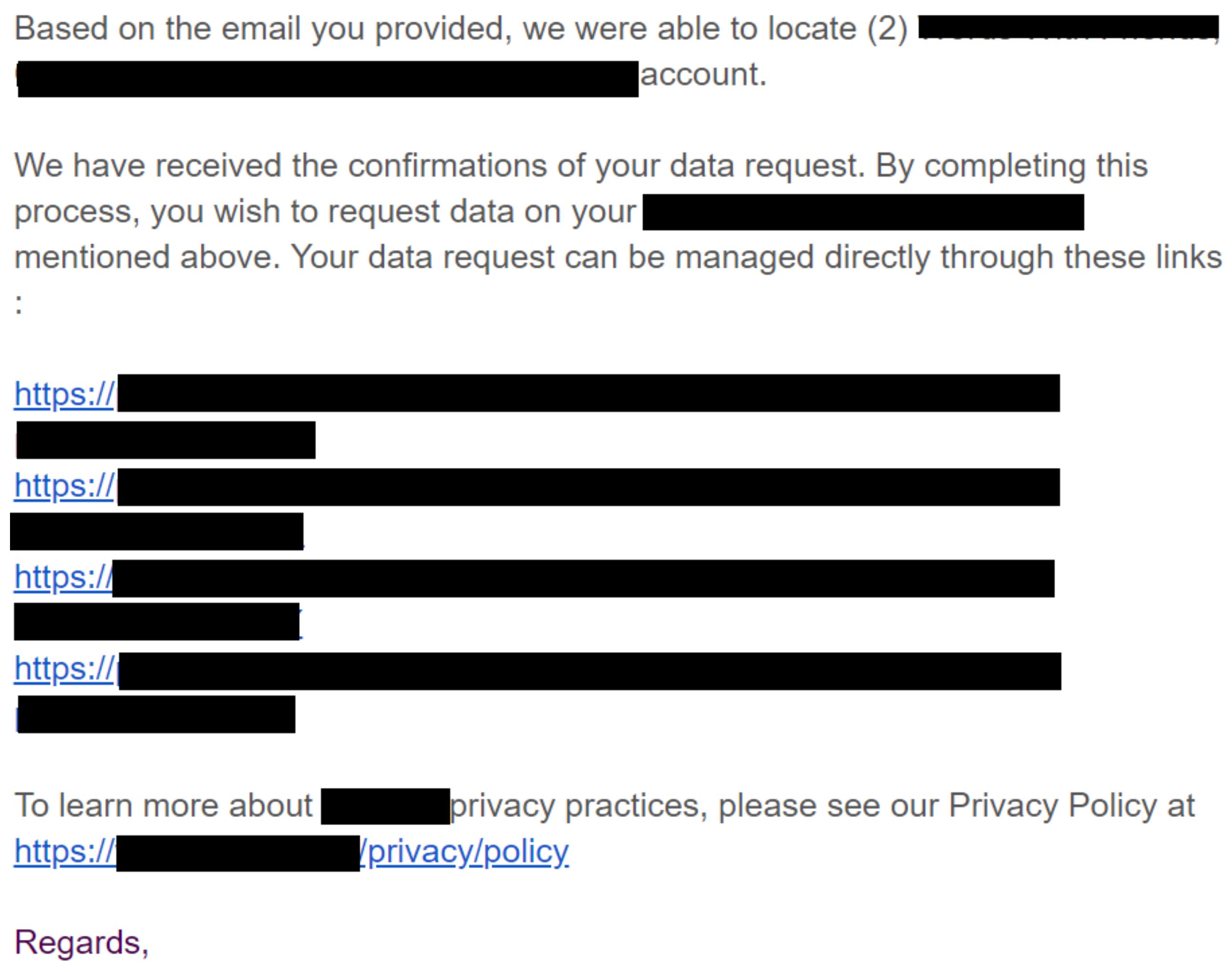
MISS [redacted] OXFORD, [redacted]

N/A
Opened
Overdraft limit
Reserve Limit
Available Balance
Last Night's Balance
Tax status (R85)

Date	Description	Money In / Out	Available Balance

Certified copy
BARCLAYS
[redacted]
[redacted] 02 2019 [redacted] [redacted]

EXFILTRATION



Based on the email you provided, we were able to locate (2) [redacted] account.

We have received the confirmations of your data request. By completing this process, you wish to request data on your [redacted] mentioned above. Your data request can be managed directly through these links :

https://[redacted]
https://[redacted]
https://[redacted]
https://[redacted]

To learn more about [redacted] privacy practices, please see our Privacy Policy at https://[redacted]/privacy/policy

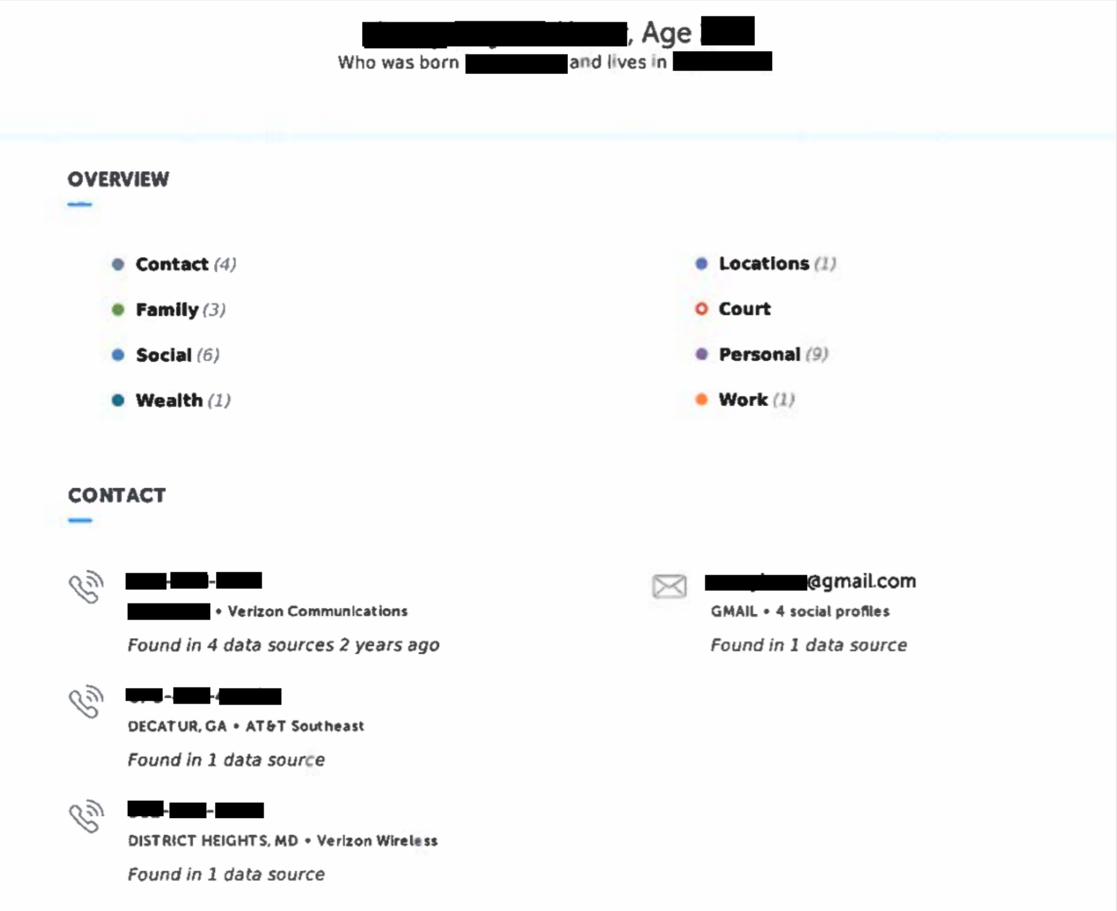
Regards,

Exfiltration: Low Sensitivity (19 instances)

Data Brokers & Advertising
(e.g. criminal history)

Account Profiles & Enumeration
(e.g. usernames)

Simple Behavioral Data
(e.g. movie bookings)



[redacted], Age [redacted]
Who was born [redacted] and lives in [redacted]

OVERVIEW

- ● **Contact** *(4)*
- ● **Family** *(3)*
- ● **Social** *(6)*
- ● **Wealth** *(1)*
- ● **Locations** *(1)*
- ○ **Court**
- ● **Personal** *(9)*
- ● **Work** *(1)*

CONTACT

☎ [redacted]-[redacted]-[redacted]
[redacted] • Verizon Communications
Found in 4 data sources 2 years ago

☎ [redacted]-[redacted]-[redacted]
DECATUR, GA • AT&T Southeast
Found in 1 data source

☎ [redacted]-[redacted]-[redacted]
DISTRICT HEIGHTS, MD • Verizon Wireless
Found in 1 data source

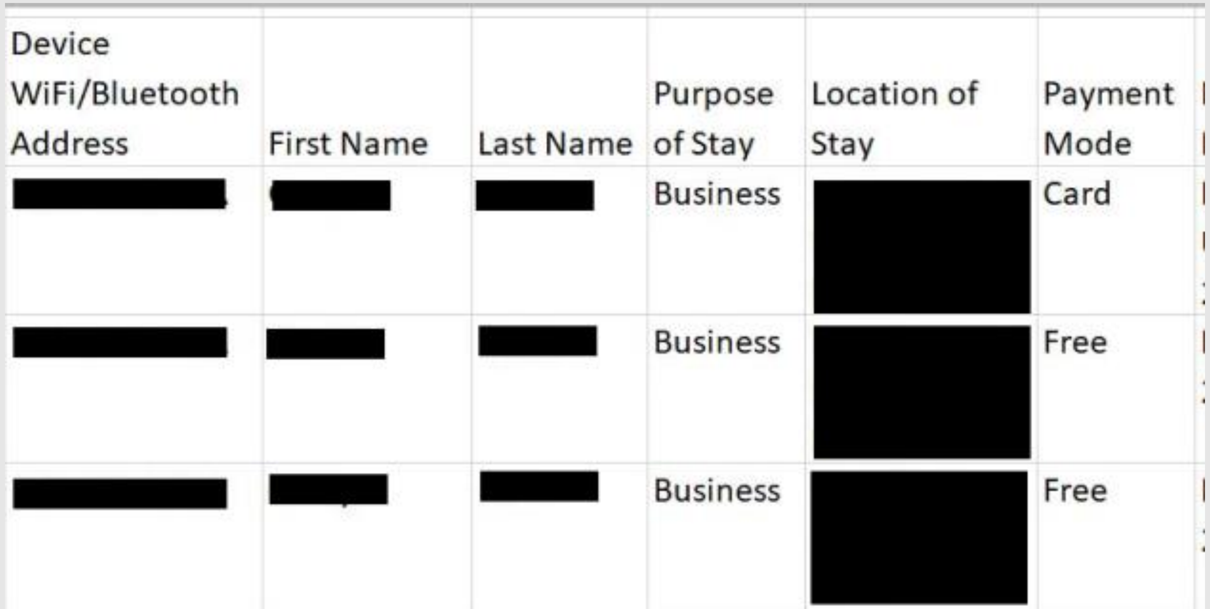
✉ [redacted]@gmail.com
GMAIL • 4 social profiles
Found in 1 data source

Exfiltration: Medium Sensitivity (48 instances)

Unique Behavioral Data
(e.g. past rail tickets)

Weak Identifiers
(e.g. phone numbers)

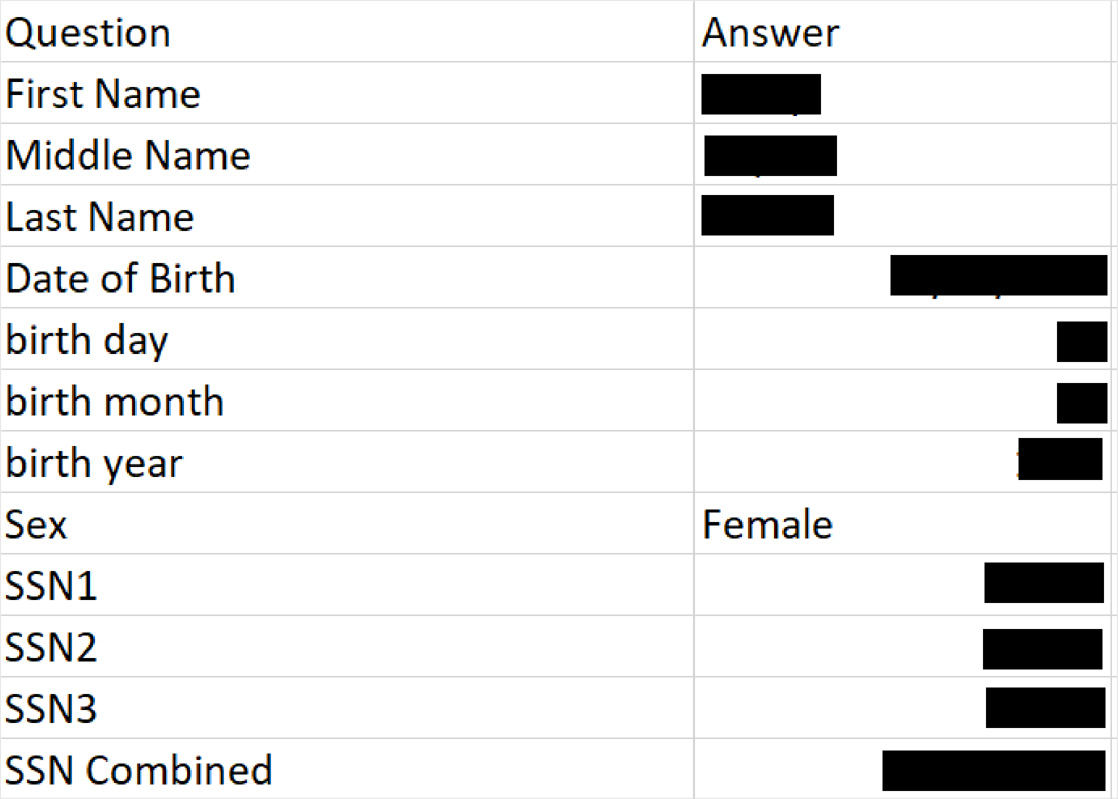
Device and Location Data
(e.g. MAC/IP)



Device WiFi/Bluetooth Address	First Name	Last Name	Purpose of Stay	Location of Stay	Payment Mode
[redacted]	[redacted]	[redacted]	Business	[redacted]	Card
[redacted]	[redacted]	[redacted]	Business	[redacted]	Free
[redacted]	[redacted]	[redacted]	Business	[redacted]	Free

Exfiltration: High Sensitivity (10 instances)

Strong Identifiers
(e.g. SSN)



Question	Answer
First Name	[redacted]
Middle Name	[redacted]
Last Name	[redacted]
Date of Birth	[redacted]
birth day	[redacted]
birth month	[redacted]
birth year	[redacted]
Sex	Female
SSN1	[redacted]
SSN2	[redacted]
SSN3	[redacted]
SSN Combined	[redacted]

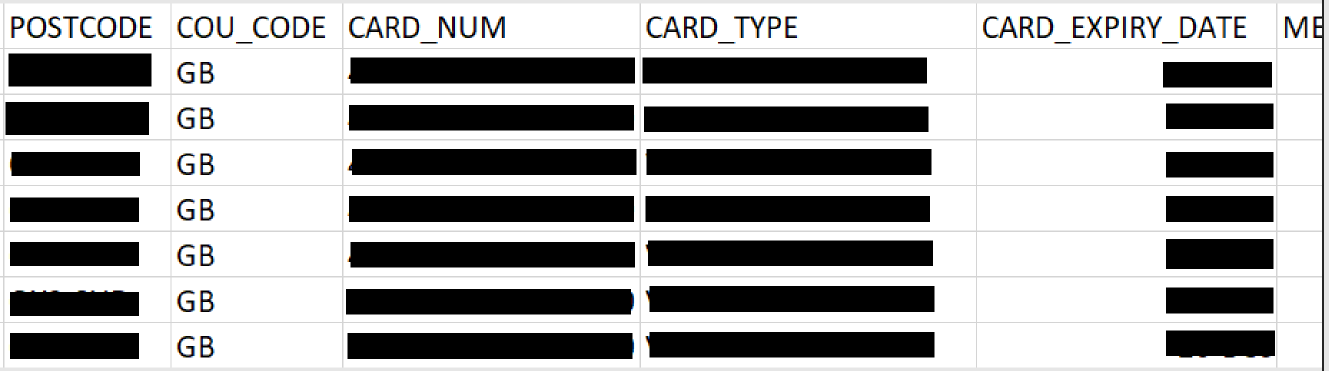
Exfiltration: High Sensitivity (10 instances)

Strong Identifiers

(e.g. SSN)

Financial Data

(e.g. CC digits)



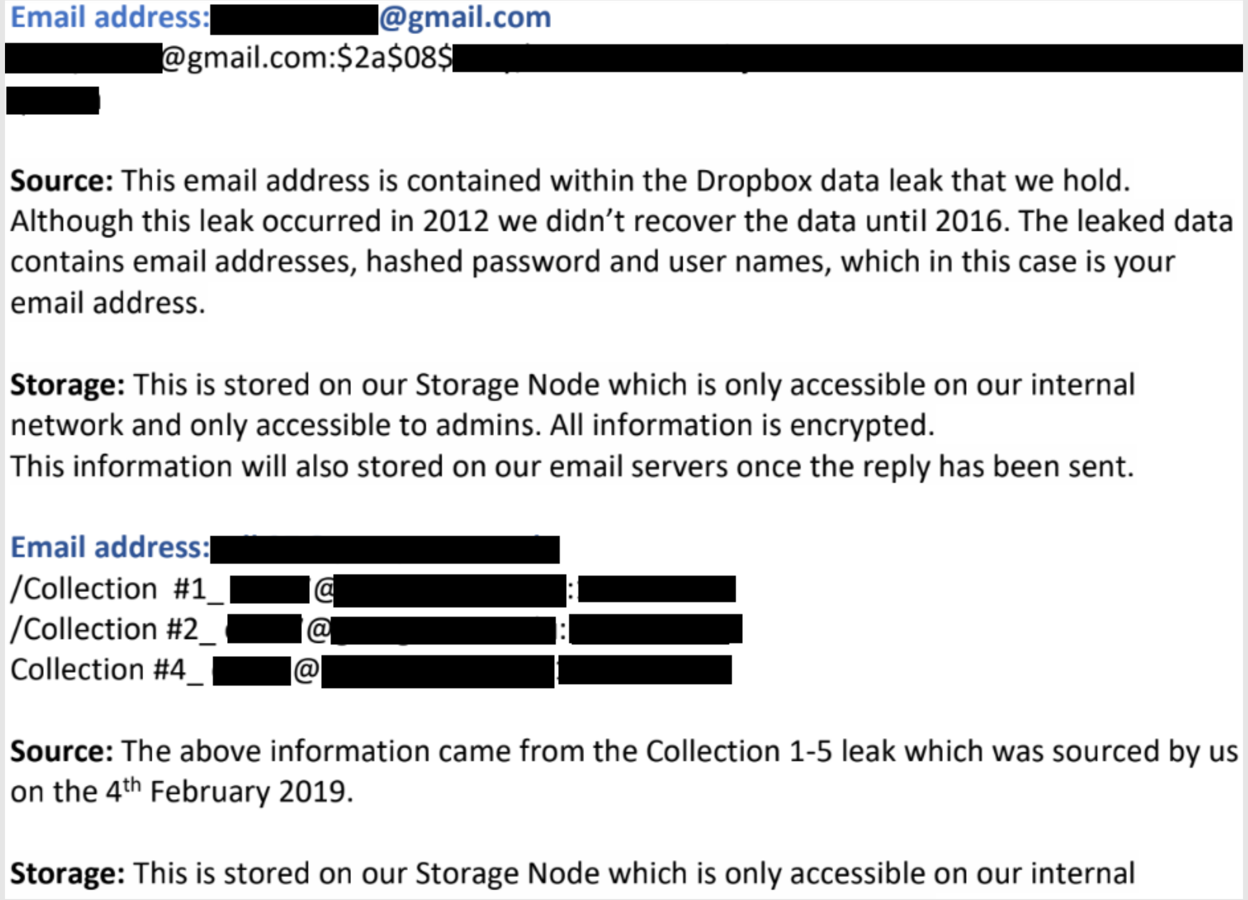
POSTCODE	COU_CODE	CARD_NUM	CARD_TYPE	CARD_EXPIRY_DATE	ME
[redacted]	GB	[redacted]	[redacted]	[redacted]	
[redacted]	GB	[redacted]	[redacted]	[redacted]	
[redacted]	GB	[redacted]	[redacted]	[redacted]	
[redacted]	GB	[redacted]	[redacted]	[redacted]	
[redacted]	GB	[redacted]	[redacted]	[redacted]	
[redacted]	GB	[redacted]	[redacted]	[redacted]	
[redacted]	GB	[redacted]	[redacted]	[redacted]	

Exfiltration: High Sensitivity (10 instances)

Strong Identifiers
(e.g. SSN)

Financial Data
(e.g. CC digits)

Credentials
(e.g. passwords and hashes)



Email address: [redacted]@gmail.com
[redacted]@gmail.com:$2a$08$[redacted]

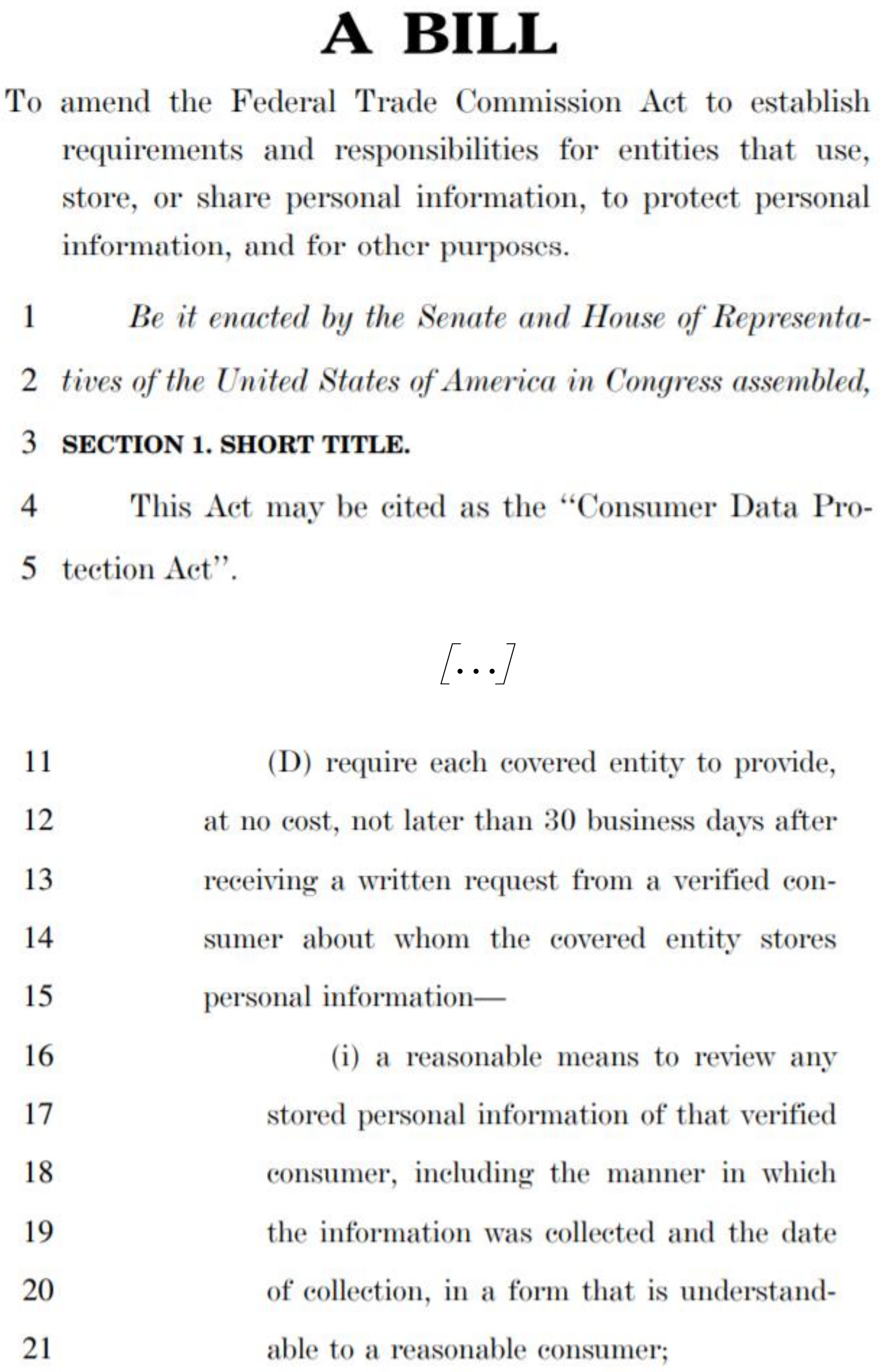
Source: This email address is contained within the Dropbox data leak that we hold. Although this leak occurred in 2012 we didn't recover the data until 2016. The leaked data contains email addresses, hashed password and user names, which in this case is your email address.

Storage: This is stored on our Storage Node which is only accessible on our internal network and only accessible to admins. All information is encrypted.
This information will also stored on our email servers once the reply has been sent.

Email address: [redacted]
/Collection #1_ [redacted]@[redacted]:[redacted]
/Collection #2_ [redacted]@[redacted]:[redacted]
Collection #4_ [redacted]@[redacted]:[redacted]

Source: The above information came from the Collection 1-5 leak which was sourced by us on the 4th February 2019.

Storage: This is stored on our Storage Node which is only accessible on our internal



A BILL

To amend the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information, to protect personal information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Consumer Data Protection Act”.

[. . .]

(D) require each covered entity to provide, at no cost, not later than 30 business days after receiving a written request from a verified consumer about whom the covered entity stores personal information—

(i) a reasonable means to review any stored personal information of that verified consumer, including the manner in which the information was collected and the date of collection, in a form that is understandable to a reasonable consumer;

REMEDIATION

Suggested Fixes: Companies

- Require account login if available
- Outsource eIDV if beyond internal capabilities
- Just say no to suspicious GDPR requests

Suggested Fixes: Legislators

- Re-assure companies that they can reject requests in good-faith
- Clarify appropriate forms of identity
- Provide government-mediated identity verification services

Suggested Fixes: Individuals

- Be pro-active about data hygiene
- Ask about past GDPR requests in your name
- Don’t trust knowledge-based authentication from unsolicited calls

Privacy laws should enhance privacy, not endanger it.

Questions? james@pavursec.com

Black Hat Sound Bytes

1. Poorly considered privacy legislation can actually endanger privacy.

2. The GDPR can be abused by social engineers to steal sensitive information through Right of Access requests.

3. Adversarial audits of privacy laws can uncover exploitable security bugs in “development” rather than “production.”