LegalExpert.co.uk
WE CAN GIVE YOU LEGAL ADVICE & GUIDANCE

A Legal Expert report

Police Force Data Breaches

An analysis of Freedom of Information requests

TABLE OF CONTENTS

DEFINITIONS

Some police forces don't have a recording category for data breaches. Some information provided was based on 'data security incidents'. The two terms are clarified below.

Data security incidents: According to some police forces, this might not necessarily mean 'personal data breach'.

Personal data breach: The Information Commissioner's Office (ICO) defines a data breach as a breach of security causing the unlawful or accidental destruction, alteration, loss, unauthorised disclosure of, or access to, personal information. Personal data breaches can be deliberate or accidental.

AIMS

Police forces in the UK play a significant part in tackling cyber security issues. LegalExpert's Freedom Of Information (FOI) request aimed to find out the number of data breaches committed by police forces and what the causes of the data breaches were. LegalExpert also requested information on whether these incidents led to civil legal action to understand the cost of data breaches on police forces.

METHODOLOGY

LegalExpert submitted FOI requests to 43 territorial police forces in England and Wales, the national police force in Scotland, and 3 specialist police forces. 3 responded together so the sample size was 44. The timescale to respond to an FOI request is usually within 20 working days. However, given the scope of the information requested, some police forces took longer to respond.

KEY INDUSTRY FACTS

£15.88 billion

funding for police forces in England and Wales

£1.299 billion

funding for Police Scotland

135,301 FTE officers

(full-time equivalent) in England and Wales police forces

17,117 FTE officers

in Police Scotland

63%

of the public trust the police in general

Source: YouGov

56%

of the public trust individual officers

Source: YouGov

LegalExpert.co.uk
WE CAN GIVE YOU LEGAL ADVICE & GUIDANCE

WHAT IS THE VALUE OF CYBER SECURITY TO POLICE FORCES?

Police forces across the UK store large quantities of personal data about their employees and some members of the public, including witnesses, suspects and criminals. Furthermore, police forces can also hold special category data, such as genetic and biometric data and
data revealing racial or ethnic origin. They also hold criminal offence data, which requires extra protection.

Subsequently, police data can be valuable for cybercriminals and cyber terrorists, who may use the information to coerce police forces financially.

Failing to address the causes of data breaches could significantly damage the reputation of police in the UK and may also seriously undermine national security. As cyber security incidents continue to rise, it is crucial that police forces effectively tackle the current and potential risks of data breaches.

CYBER CRIME IN THE UK

£3.1bn

This year, cyber crime has cost the UK £3.1bn - an increase of £1.8bn compared to 2021.

416,839

The number of cyber crime reports made so far in 2022 - an increased of 44% compared to 2021.

141.6k

The number of reports made for consumer fraud, which is the most common cyber crime this year.

Source: National Fraud Intelligence

FINDINGS

Out of all the police forces we contacted, 89% responded to our FOIs. While 11 forces provided complete responses, 24 partially answered the FOI request, 4 forces responded but did not provide any information, and 5 did not respond. For those police forces that provided exact statistics for the number of suspected data breaches or data security incidents that had occurred between 2019 and November 2021, we were able to find there had been around 13,332 incidents.

Out of the police forces that responded, we found that:

- There were 13,332 suspected data breaches or security incidents (although this number is likely to be higher given not all forces were able to state the specific number)
- 90% had dealt with at least 1 suspected data security incident
- 59% had identified over 100 suspected data breach or data security incidents
- Email misuse, including sending unsecured emails and emails being sent in error, was the most common security incident affecting 28% of respondent police forces
- Lost or stolen device or technological assets closely followed, affecting 26% of respondent police forces
- Around 51% confirmed that they'd received some form of civil legal action in regards to data security incidents, indicating data breaches are costing police forces

The following requests were made:

- The number of data breaches committed by *specified police force* between 2019 up to the date of this request (November 2021).
- The cause of these data breaches, such as emails being sent in error, or devices being lost, as well as any cyber attacks.
- What types of information were exposed in the breaches?
- Had *specified police force* been subjected to any civil legal action in relation to any of these breaches? If so, can you advise how many have been settled, abandoned or the number ongoing?

The table below shows which police forces answered each request.

R1	R2	R3	R4
Avon and Somerset Police Bedfordshire Police Cambridgeshire Constabulary Cheshire Constabulary City of London Police Civil Nuclear Constabulary Cleveland Police Derbyshire Constabulary Devon and Cornwall Police Dorset Police Durham Constabulary Dyfed-Powys Police Greater Manchester Police Gwent Police Hertfordshire Constabulary Kent and Essex Police (Joint response) Lancashire Constabulary Leicestershire Police Lincolnshire Police Merseyside Police Ministry of Defence Police Norfolk and Suffolk Constabulary (Joint response) Northumbria Police Police Scotland Staffordshire Police Surrey Police Sussex Police West Mercia Police West Yorkshire Police Wiltshire Police	British Transport Police City of London Police Civil Nuclear Constabulary Derbyshire Constabulary Devon and Cornwall Police Dorset Police Durham Constabulary Gwent Police Kent and Essex Police (Joint response) Lancashire Constabulary Lincolnshire Police Merseyside Police Ministry of Defence Police Northumbria Police Police Scotland Staffordshire Police Surrey Police Sussex Police West Yorkshire Police	City of London Police Civil Nuclear Constabulary Cleveland Police Derbyshire Constabulary Durham Constabulary Gwent Police Kent and Essex Police (Joint response) Lancashire Constabulary Lincolnshire Police Merseyside Police Ministry of Defence Police Northumbria Police Surrey Police Sussex Police	City of London Police Civil Nuclear Constabulary Cleveland Police Derbyshire Constabulary Durham Constabulary Dyfed-Powys Police Gwent Police Kent and Essex Police (Joint response) Lancashire Constabulary Lincolnshire Police Merseyside Police Metropolitan Police North Wales Police Northumbria Police Police Scotland South Yorkshire Police Staffordshire Police Surrey Police Sussex Police Thames Valley Police (joint with Hampshire Constabulary)
Total: 30	Total: 19	Total: 14	Total: 20

Before discussing the findings, it is worth noting why some police forces did not answer the FOI requests:

Some requests were denied because, under Section 12 (1) of the Freedom of Information Act, obtaining the information would exceed the appropriate cost and time limit. The cost limit is currently set at £450, while the time limit is set at 18 hours of staff work.

Some police forces said the request would exceed the appropriate limit as the information requested was not centrally recorded. Therefore, it was not readily available in an easily retrievable format and would have required a manual review of sometimes hundreds of incident reports.

Police forces who responded to the FOI but would not confirm what types of data were exposed said that revealing this information may breach the data subject's interests or fundamental rights and freedoms.

Concerning cyber attacks, some police forces refused to provide information on how many incidents there had been in fear of adversely impacting the operational effectiveness of the force.

Furthermore, some police forces said that releasing data on cyber attacks may compromise any tactical advantage police could have.

South Wales Police, who denied all the requested information, highlighted that based on intelligence at the time of the response, the UK threat level from international terrorism was severe, meaning a terrorist attack was likely. Subsequently, revealing information on data breaches and cyber attacks could undermine national security and leave the UK at risk of terrorism. The force concluded that safeguarding national security mattered more than revealing the requested data.

Police forces who did not respond are listed below:

- Cumbria Constabulary
- Northamptonshire Police
- North Yorkshire Police
- Nottinghamshire Police
- Warwickshire Police

WHAT LEGAL EXPERT SAYS

Our data breach team at Legal Expert have almost 10 years of experience dealing with and settling data breach claims between us.

We are already dealing with a significant number of cases against various polices constabularies in England and Wales as a result of their repeated failures to adhere to the GDPR and data protection legislation. Due to the vast amounts of sensitive information the police process, many cases we deal with are severe and can often to lead to significant distress and psychological injury to our clients. The figures show that the majority of cases involve personal and sensitive information being sent to an incorrect recipient, lost or stolen. Often individuals subject to investigation can feel embarrassment, distress and anxiety if this information is shared with unauthorised third parties.

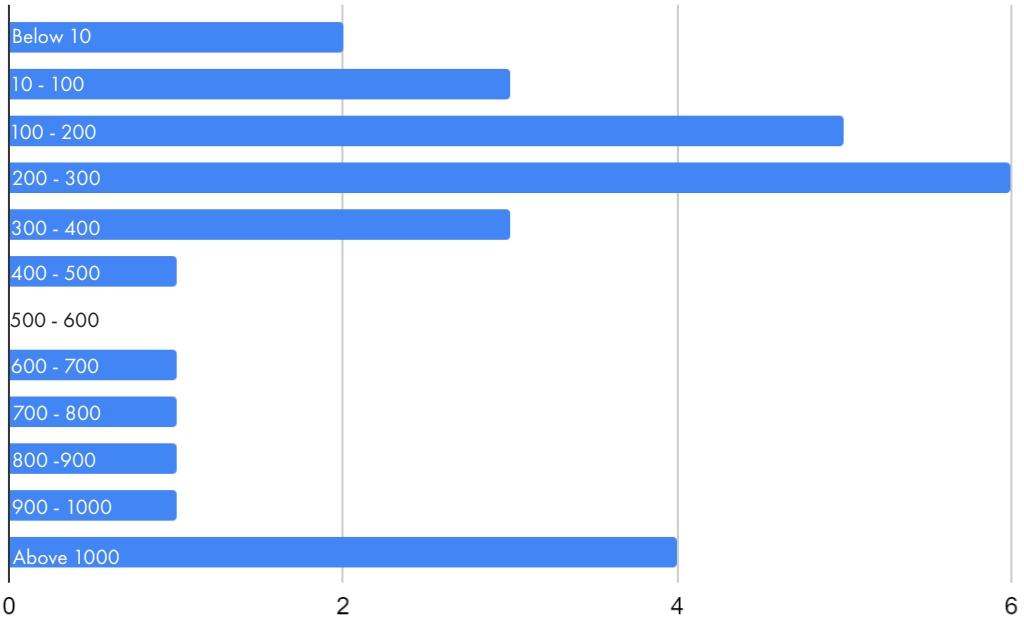
We feel it is important that people know and understand their data protection rights and when they would be eligible to make a claim for compensation. In one particular case damages in the sum of £19,000.00 were obtained on behalf of a client whose confidential bail documents were mistakenly addressed to their neighbour. This resulted in a recognised psychological disorder for the client which required expert treatment and attracted this substantial sum of damages.

We would strongly encourage anyone who has, or suspects they have, been a victim of any data breach incident involving the police, regardless of how minor, to seek legal advice to discuss their claim further.

DATA BREACHES OVERALL

LegalExpert reached out to police forces to determine how many data breach incidents there had been from 2019 to November 2021. Using responses from police forces that answered the FOIs, we found that 90% had recorded at least one suspected data breach or data security incident from 2019 to November 2021. The chart below depicts the volume of suspected security incidents that police forces experienced during this time

BREAKDOWN OF POLICE FORCES THAT REPORTED DATA BREACHES



Data for Chart One:

Below ten breaches: Civil Nuclear Constabulary, Ministry of Defence Police
10 – 100: City of London Police, Northumbria Police, Staffordshire Police
100 – 200: Bedfordshire Police, Cambridgeshire Constabulary, Cleveland Police, Gwent Police, Merseyside Police
200 – 300: Dyfed-Powys Police, Greater Manchester Police, Leicestershire Police, Lincolnshire Police, Surrey Police, Wiltshire Police
300 – 400: Durham Constabulary, Hertfordshire Constabulary, Sussex Police
400 – 500: Dorset Police
500 – 600: None
600 – 700: West Yorkshire Police
700 – 800: Suffolk Constabulary (joint with Norfolk Constabulary)
800 – 900: Devon and Cornwall Police
900 – 1000: Cheshire Constabulary
1000 +: Kent Police (joint with Essex Police), Lancashire Constabulary, Police Scotland, West Mercia Police

DATA BREACHES BY POLICE FORCE

The table below depicts exactly how many suspected data breaches or security incidents occurred from 2019 to November 2021. The table also states how many officers work for each police force and the size of the land covered by each police force too.

Figures as of May 2022.

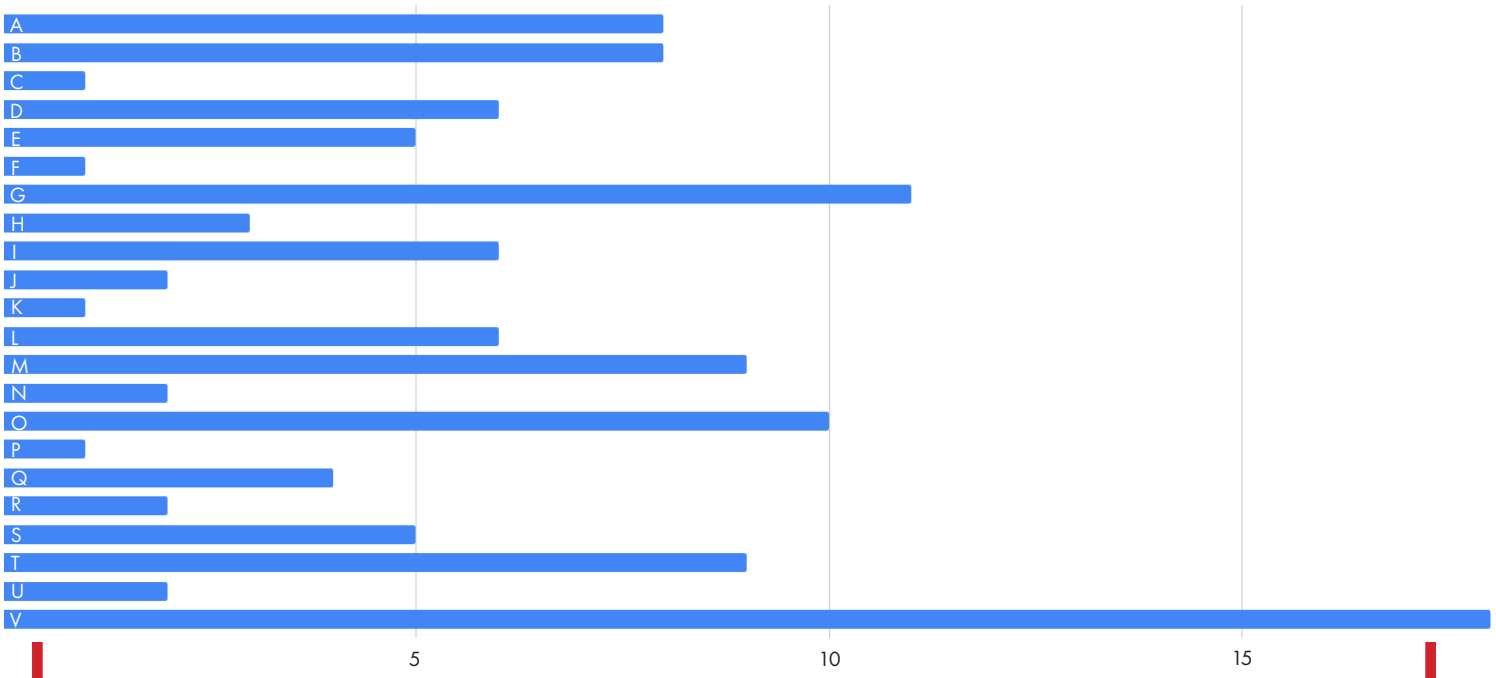
Police Force	Notes	How Many Suspected Data Breach Or Data Security Incidents?
Avon and Somerset Police	• 2,997 officers • Covers 4,784 km2	Over 600 suspected cases (not specified)
Bedfordshire Police	• 1,335 officers • 1,235 km2	162
British Transport Police	• 2,902 officers	N/A
Cambridgeshire Constabulary	• 1,620 officers • 3,395 km2	183
Cheshire Constabulary	• 2,149 officers • 2,450 km2	956
Civil Nuclear Constabulary	• 1,310 officers	3
City of London Police	• 849 officers • 2.6 km2	27
Cleveland Police	• 1,414 officers • 596 km2	123
Cumbria Constabulary	• 1,251 officers • 6,810 km2	N/A
Derbyshire Constabulary	• 1,882 officers • 3,000 km2	304
Devon and Cornwall Police	• 3,264 officers • 10,360 km2	869

Dorset Police	• 1,283 officers • 2,652 km2	479
Durham Constabulary	• 1,214 officers • 2,232 km^2	396
Dyfed-Powys Police	• 1,182 officers • 10,847 km^2	212
Essex Police (joint with Kent Police)	• 3,415 officers (Essex) • 3,678 km^2 (Essex)	1,356 (See Essex Police)
Gloucestershire Constabulary	• 1,216 officers • 2,696 km^2	N/A
Greater Manchester Police	• 7,086 officers • 1,295 km^2	243
Gwent Police	• 1,362 officers • 1,554 km^2	178
Hampshire Constabulary (joint with Thames Valley Police)	• 3,040 officers • 4,178 km^2	N/A
Hertfordshire Constabulary	• 2,199 officers • 1,642 km^2	329
Humberside Police	• 2,053 officers • 3,512 km^2	N/A
Kent Police (joint with Essex Police)	• 3,911 officers (Kent) • 3,737 km^2 (Kent)	1,356 (See Essex Police)
Lancashire Constabulary	• 3,131 officers • 3,079 km^2	1,317
Leicestershire Police	• 2,201 officers • 2,538 km^2	296
Lincolnshire Police	• 1,136 officers • 5,936 km^2	204
Merseyside Police	• 3,940 officers • 647 km^2	111
Metropolitan Police Service	• 32,954 officers • 1,578 km^2	N/A
Ministry of Defence Police	• 2,594 officers	7
Norfolk Constabulary (Joint response with Suffolk Constabulary)	• 1,735 officers (Norfolk) • 5,379 km^2 (Norfolk)	Close to 800 incidents (See Suffolk Constabulary)

North Wales Police	• 1,591 officers • 6,151 km²	N/A
Northamptonshire Police	• 1,348 officers • 2,367 km²	N/A
Northumbria Police	• 3,416 officers • 5,553 km²	38
North Yorkshire Police	• 1,487 officers • 8,309 km²	N/A
Nottinghamshire Police	• 2,182 officers • 2,160 km²	N/A
Police Scotland	• 17,170 officers • 72,955 km²	2,809
South Wales Police	• 3,174 officers • 2,103 km²	N/A
South Yorkshire Police	• 2,745 officers • 1,554 km²	N/A
Staffordshire Police	• 1,749 officers • 2,590 km²	77
Suffolk Constabulary (joint with Norfolk Constabulary)	• 1,286 officers (Suffolk) • 3,797 km² (Suffolk)	Close to 800 incidents (See Norfolk Constabulary)
Surrey Police	• 2,086 officers • 1,663 km²	231
Sussex Police	• 2,838 officers • 3,781 km²	310
Thames Valley Police (joint with Hampshire Constabulary)	• 4,401 officers • 5,740 km²	N/A
Warwickshire Police	• 1,060 officers • 1,976 km²	N/A
West Mercia Police	• 2,277 officers • 7,428 km²	1,252
West Midlands Police	• 7,186 officers • 901 km²	N/A
West Yorkshire Police	• 5,580 officers • 2,020 km²	641
Wiltshire Police	• 1,078 officers • 3,485 km²	219

CAUSES OF POLICE DATA SECURITY INCIDENTS

There were 21 categories of security incidents that were identified in our FOI responses.



A - Disclosure to incorrect recipient via email
B - Disclosure to incorrect recipient via post
C - Cyber attacks
D - Data stored unsecurely/incorrectly
E - Device misuse
F - Document misuse
G - Email misuse (including unsecured email and email sent in error)
H - Failure to redact
I - Force system misuse (including unauthorised access)
J - Incorrect information disclosed
K - Unsecure disposal of data
L - Loss of ID/warrant cards
M - Lost or stolen data
N - Loss of seized property
O - Lost or stolen devices/technological assets
P - Malware
Q - Physical security breach
R - Social media misuse
S - Software/system failings
T - Unauthorised access or disclosure
U - Verbal disclosure
V - Security Incidents (Cyber and Non-Cyber) not disclosed

The table below provides information on the chart above, including the different categories of security incidents and the number of police forces that reported it as an issue. It is important to note that not all listed security incidents directly caused a data breach.

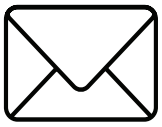
Note: Police forces who are yet to respond are not featured in these statistics.

Security Incidents (Cyber and Non-Cyber)	Number of Police Forces
Disclosure to incorrect recipient via email	8 - City of London Police; Derbyshire Constabulary; Durham Constabulary; Lancashire Constabulary; Lincolnshire Police; Merseyside Police; Northumbria Police; Sussex Police
Disclosure to incorrect recipient via post	8 - Civil Nuclear Constabulary; Derbyshire Constabulary; Lancashire Constabulary; Lincolnshire Police; Merseyside Police; Northumbria Police; Surrey Police; Sussex Police
Cyber attacks	1 - Sussex Police. West Yorkshire Police confirmed they had no cyber attacks. It's worth noting that many forces refused to provide information in fear of compromising their cyber security.
Data stored unsecurely/incorrectly	6 - British Transport Police; Derbyshire Constabulary; Gwent Police; Merseyside Police; Ministry of Defence; Northumbria Police
Device misuse	5 - Durham Constabulary; Kent and Essex Police; Lincolnshire Police; Staffordshire Police; West Yorkshire Police
Document misuse	1 - Kent and Essex Police
Email misuse (including unsecured email and email sent in error)	11 - Devon and Cornwall Police; Dorset Police; Gwent Police; Kent and Essex Police; Lancashire Constabulary; Lincolnshire Police; Ministry of Defence; Police Scotland; Staffordshire Police; Surrey Police, West Yorkshire Police
Failure to redact	3 - Derbyshire Constabulary; Lincolnshire Police; Surrey Police
Force system misuse (including unauthorised access)	6 - Derbyshire Constabulary; Durham Constabulary; Gwent Police; Kent and Essex Police; Lincolnshire Police; Merseyside Police

Incorrect information disclosed	2 - Lincolnshire Police; Staffordshire Police
Unsecure disposal of data	1 - Derbyshire Constabulary
Loss of ID/warrant cards	6 - Civil Nuclear Constabulary; British Transport Police; Devon and Cornwall Police; Dorset Police; Durham Constabulary; Lancashire Constabulary
Lost or stolen data	9 - British Transport Police; City of London Police; Derbyshire Constabulary; Devon and Cornwall Police; Dorset Police; Durham Constabulary; Lincolnshire Police; Staffordshire Police; Sussex Police
Loss of seized property	2 - Devon and Cornwall Police; Dorset Police
Lost or stolen devices/technological assets	10 - Civil Nuclear Constabulary; Derbyshire Constabulary; Devon and Cornwall Police; Dorset Police; Durham Constabulary; Lancashire Constabulary; Lincolnshire Police; Staffordshire Police; Surrey Police; Sussex PolicePolice, West Yorkshire Police
Malware	1 - Lincolnshire Police
Physical security breach	4 - British Transport Police; Devon and Cornwall Police; Dorset Police; Police Scotland
Social media misuse	2 - Ministry of Defence; Kent and Essex Police
Software/system failings	5 - British Transport Police; Dorset Police; Kent and Essex Police; Lincolnshire Police; Sussex Police
Unauthorised access or disclosure	9 - Civil Nuclear Constabulary; Derbyshire Constabulary; Devon and Cornwall Police; Dorset Police; Kent and Essex Police; Lancashire Constabulary; Lincolnshire Police; Police Scotland; West Yorkshire Police
Verbal disclosure	2 - Derbyshire Constabulary; Northumbria Police
Security Incidents (Cyber and Non-Cyber) not disclosed	18 - Avon and Somerset Police, Bedfordshire Police, Cheshire Constabulary, Cambridgeshire Constabulary, Cleveland Police, Dyfed-Powys Police, Gloucestershire Constabulary, Greater Manchester Police, Hertfordshire Constabulary, Leicestershire Police, Metropolitan Police Service, Norfolk and Suffolk Constabulary, North Wales Police, South Wales Police, South Yorkshire Police, Hampshire Constabulary and Thames Valley Police, West Mercia Police, Wiltshire Police

DISCLOSURE TO INCORRECT RECIPIENT VIA EMAIL

Sending an email to the wrong person, whether internally or externally, may cause major issues for police forces since emails may contain sensitive data. Our research found that this wasn't an uncommon cause of data breaches in police forces, with 8 admitting to such incidents.



Some police forces reported accidentally copying incorrect recipients into email exchanges. For example, Lincolnshire Police sent phone data and case details to the wrong person.

This type of breach seemed most common for Derbyshire Constabulary, recording 79 incidents.

DISCLOSURE TO INCORRECT RECIPIENT VIA POST

Sending information to the wrong person by post wasn't an uncommon cause of data breaches. A total of 8 forces were found to have done this.

This type of incident can be caused by human error and may compromise the security of personal data. For example, Civil Nuclear Constabulary had posted some pension statements to the wrong address. In an incident with Merseyside Police, documentation for an individual was left at a neighbour's house.

CYBER ATTACKS

Cyber attacks can be defined as a deliberate attempt to gain unauthorised access to computer systems and networks to expose, modify or steal data.

Most police forces who responded to our FOI refused to provide data on cyber attacks in fear of compromising their cyber security. Some forces, including Police Scotland, feared that giving this information would harm their operational effectiveness. Others, such as South Wales Police, refused the request because it could undermine national security and leave the UK at risk of terrorism.

Just two forces responded: West Yorkshire Police, who confirmed they had had no cyber attacks, and Sussex Police, who reported 7 incidents.

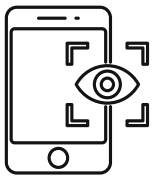
DATA STORED UNSECURELY/INCORRECTLY

Personal data that is not securely or correctly stored could pose a significant risk to the data subject, particularly if it is left in a place where it may be wrongly disposed of or possibly stolen.

Gwent Police had an incident in which hard copy data was left unattended. Merseyside Police had dispatched unsealed letters.

DEVICE MISUSE

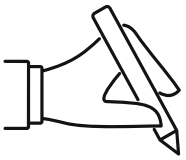
Device misuse may occur when a device is used without permission or used for a different purpose than it is intended. This type of breach may include computer misuse or unauthorised access to hard disks.



The rate of this type of incident was low amongst the forces that reported it happening.

DOCUMENT MISUSE

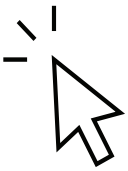
Like device misuse, document misuse accounts for unauthorised access to documents and may lead to personal data being tampered with, destroyed or stolen.



It was just Kent and Essex Police that reported this type of incident, making it one of the least common causes of suspected data breaches or incidents.

EMAIL MISUSE

Email misuse can occur when email accounts are accessed or used without permission and may lead to incorrect information being sent out or the wrong recipients receiving confidential information. This type of incident may involve emails being sent on unsecure servers, sensitive content being sent via unsecure means, or emails being sent in error.



A total of 11 police forces reported email misuse incidents, making it the most common cause of suspected data breaches or security incidents. Lancashire Constabulary reported 817 instances of email misuse.

FAILURE TO REDACT

Documents are redacted to protect information that is considered confidential. The Information Commissioner's Office says that personal data may sometimes be redacted by police when making information available under an FOI or responding to a subject access request under the Data Protection Act 2018.

3 police forces reported failure to redact, although the volume of these incidents appeared to be in the single figures, indicating that it was not too much of a problem for police.

FORCE SYSTEM MISUSE (INCLUDING UNAUTHORISED ACCESS)

Police officers may have access to the Police National Computer and the Force Intelligence Systems. If officers use force computer systems without consent or for reasons other than work, they may be prosecuted for criminal offences and could face misconduct proceedings. These systems store a large amount of sensitive data, such as a person's criminal conviction record. Therefore officers should use the system correctly.

6 police forces recorded instances of force system misuse, including Merseyside Police, where an unspecified staff member used the system for personal use.

INCORRECT INFORMATION DISCLOSED

Lancashire Constabulary and Staffordshire Police reported the disclosure of incorrect information, indicating this type of incident is not common amongst police forces.

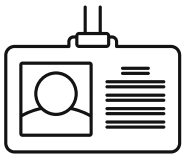
However, there were 37 recorded instances by Lancashire Constabulary, making it the second most common cause of data breach incidents for that specific force.

UNSECURE DISPOSAL OF DATA

Just 1 police force had this issue: Derbyshire Constabulary reported two instances where paperwork was not securely disposed of. While it was not a common problem for police forces, it should still be taken seriously. If personal data is not properly disposed of, it could be accessed by unauthorised parties.

LOSS OF ID/WARRANT CARDS

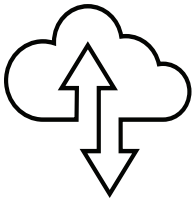
The loss of ID or warrant cards could lead to individuals impersonating police officers, posing a significant risk to the force's reputation and the public's safety.



6 police forces reported the loss of ID or warrant cards. It was a relatively common incident for Devon and Cornwall Police, who recorded 163 incidents.

LOST OR STOLEN DATA

Lost or stolen data incidents occurred at 9 respondent police forces, specifically the loss or theft of paper documents containing data.



Dorset Police reported 145 incidents where this had happened, including when a CD and an employee pocket notebook containing data had gone missing.

LOSS OF SEIZED PROPERTY

Loss of seized property was a type of data breach identified in just 2 forces: Devon and Cornwall Police and Dorset Police. However, the frequency rate was low for both forces. Seized property may also include property that is found or recovered by officers.

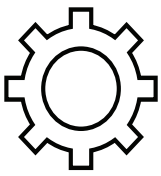
LOST OR STOLEN DEVICES/TECHNOLOGICAL ASSETS

10 forces reported this incident, indicating it was a shared issue. Assets reported lost or stolen included laptops, USB sticks and Body Worn Video cameras.

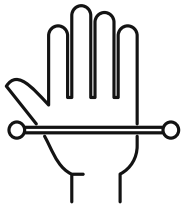
The frequency was high amongst some forces who reported the incident, including Devon and Cornwall Police (117 times) and Lancashire Constabulary (130 times).

MALWARE

Malware poses a serious threat to police force systems, given it is software designed to attack computer devices and networks. The issue was only reported by Lincolnshire Police, however.



PHYSICAL SECURITY BREACH



Physical security breach incidents happened in 4 forces, but the frequency rate was low. These types of incidents should be taken seriously by police since they may lead to data being lost or stolen. Unauthorised access may happen with outsiders from the force or staff that work in the force but should not be accessing areas beyond their means.

SOCIAL MEDIA MISUSE

Police officers may face serious disciplinary action if they do not uphold standards of professional behaviour on social media, including in private messenger applications. Just 2 forces identified social media misuse as an issue: Kent and Essex Police and the Ministry of Defence. Both forces reported the incident happening no more than twice

SOFTWARE/SYSTEM FAILINGS

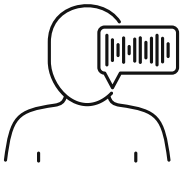
Police forces should update and secure their systems to avoid them failing. System failures may sometimes be inevitable, too, if there is a power outage for example. 5 forces identified this type of security incident. System issues were most common for Sussex Police, who reported 15 incidents.

UNAUTHORISED ACCESS OR DISCLOSURE

The unauthorised access or disclosure of information was a common issue identified by police forces. 9 forces reported this type of incident.

One force, Civil Nuclear Constabulary (CNC), revealed that in June 2020, access controls were not properly managed on a shared drive, allowing employees in another section to access the document titles, including health and safety reports. The ICO took no further action after CNC took action to identify, mitigate and contain the breach.

VERBAL DISCLOSURE



Derbyshire Constabulary and Northumbria Police were the only forces to report this incident. Verbal disclosure may happen if an officer discloses personal information to someone not authorised to hear it. It could also happen if an officer is overheard talking about personal information.

TYPES OF DATA

Police force data breaches may lead to the personal data of criminals, suspects, staff, witnesses and members of the public being exposed.

To help illustrate the different types of information that could be exposed due to police force data breach incidents, we have put together a table. The first category is personal data, and this is information that can identify someone, whether on its own or in connection with other personal data.

Some types of personal data are considered to be more sensitive. The ICO refers to this type of information as special category data, forming the table's second category.

Criminal offence data, like special category data, requires extra protection due to its sensitivity.

Personal Data/ Personal Information	Special Category Data	Criminal Offence Data
• Addresses • Contact details • Date of birth • Names • ID card • Email addresses • Financial data	• Health data • Biometric data (for ID purposes) • Genetic data • Ethnicity or race • Trade union memberships • Religion or philosophical beliefs • Political opinions • Sexual orientation • Sex life	• Criminal offence data i.e. allegations, investigations, proceedings and convictions

Lancashire Constabulary provided examples of when personal data had been breached. In one instance, medical information about a third party was inadvertently disclosed to a victim and, in another, incorrect data about an offender was shared with social services.

Lincolnshire Police also revealed how some criminal offence data had been exposed, including when an individual's offending history was seen on a police officer's mobile phone.

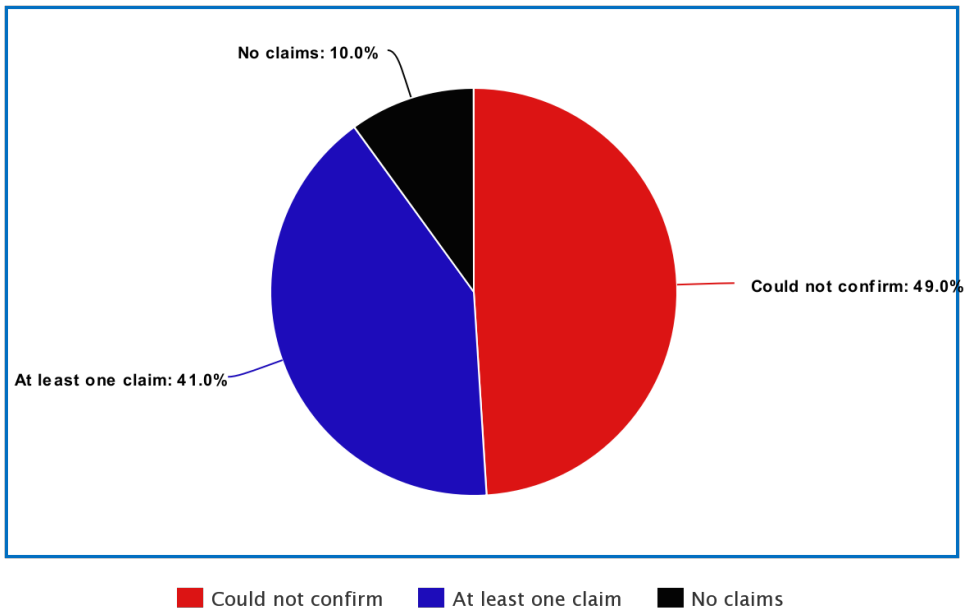
CLAIMS MADE AGAINST POLICE FORCES IN RELATION TO DATA BREACHES

Out of the respondent forces that responded to our FOI, 51% had dealt with at least 1 civil action that had resulted from a data breach incident. Many forces would not confirm if they dealt with claims because it would exceed the appropriate limit of an FOI request.

Police Force	Response	Total Claims
City of London Police	• Just 1 claim is presently being assessed	1
Civil Nuclear Constabulary	• No claims against Civil Nuclear Constabulary	0
Cleveland Police	• In 2019, Cleveland Police settled 8 claims while 2 were withdrawn • In 2020, the force received 4 claims and settled 1 • In 2021, the force received 4 claims	16
Derbyshire Constabulary	• There are 2 ongoing claims (potentially not linked to data breaches)	2
Durham Constabulary	• Just 1 claim is presently being assessed	1
Dyfed-Powys Police	• No claims against Dyfed-Powys Police	0
Gwent Police	• No claims against Gwent Police	0
Kent and Essex Police (Joint response)	• In 2019, 3 claims were settled. 4 claims remain ongoing • In 2020, 3 claims were ongoing and 1 was settled • In 2021, 1 claim was settled while 5 are ongoing	17

Lancashire Constabulary	• There have been 7 claims, 3 that were settled, 1 not pursued and 3 ongoing	7
Lincolnshire Police	• Total of 6 claims. 1 was settled	6
Merseyside Police	• There are 8 ongoing civil litigation cases, while 6 were settled	8
Metropolitan Police	• Metropolitan Police are dealing with 9 claims (though they may not relate to data breaches)	9
North Wales Police	• In 2019, North Wales Police dealt with 1 claim, which was defended • In 2020, there were 4 claims: 1 settled, 2 defended and 1 ongoing • In 2021, the force dealt with 7 claims: 5 of which are ongoing and 2 have been settled	12
Northumbria Police	• No claims against Northumbria Police	0
Police Scotland	• Police Scotland have dealt with 5 claims	5
South Yorkshire Police	• South Yorkshire Police dealt with 93 matters	93
Staffordshire Police	• A total of 9 claims: 2 were settled, 2 were not pursued, repudiated, closed or declined, 5 are ongoing	9
Surrey Police	• A total of 2 claims: 1 ongoing and 1 finalised without any payment being made	8
Sussex Police	• 1 claim had been settled	1
Thames Valley Police (joint with Hampshire Constabulary)	• In 2019, there were no claims • In 2020, there were 6 claims (2 were repudiated)	13
		TOTAL: 202

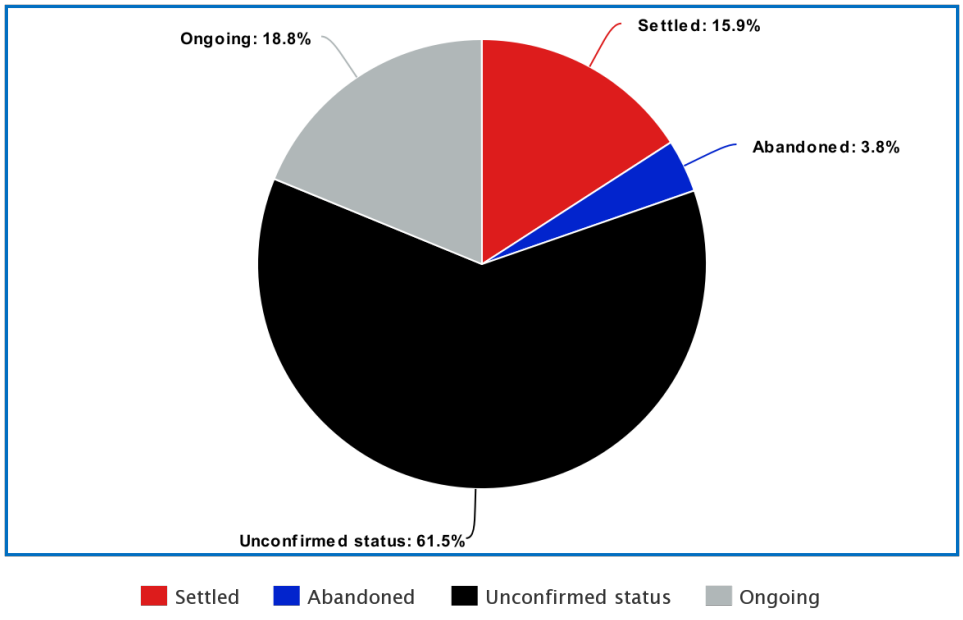
CIVIL LEGAL ACTION CLAIMS AGAINST POLICE



The findings of the police forces who provided statistics on civil legal action are included in the table and pie chart below. There were a total of 208 claims filed against several forces. However, they might not all be related to data breach claims.

Some forces, such as the Metropolitan Police, did not confirm whether they had settled the claims. However, the Met did confirm that they had also faced 72 threats of civil legal action.

Settled	Abandoned	Ongoing	Unconfirmed
40	11	47	121



LOOKING AHEAD

Police forces are facing mounting financial difficulties in the wake of the Covid-19 pandemic in 2020. Before the pandemic, funding for forces was down nearly a fifth (19%) from 2010. Despite this, forces must continue to tackle data breaches and improve cyber security. Police forces may not only endure financial costs as a result of data breaches but also put their reputation at risk.

Our FOI analysis suggests that data breaches are a prominent issue for police forces and that, given the number of claims made against forces, they are, potentially, a financial burden. Therefore, more needs to be done across the sector to improve cyber security and data protection.

Based on the data analysed, the biggest causes of security incidents seems to be associated with human error. Email errors in particular featured prominently in responses. Issues like this could be resolved through more modern email systems with security checks in place, such as warnings when sending out attachments, and the ability to recall emails within a certain period of time. Combined with greater training on data security risks, the number of incidents could fall.

However, police forces are beginning to make the right changes. The NPCC National Cybercrime Programme revealed that every police force in England and Wales has a dedicated cybercrime team. Before 2019, just 31% of forces were equipped with specialised units that dealt with cyber security incidents.

ABOUT LEGAL EXPERT

Legal Expert is a trading name of JF Law Limited, a law firm regulated by the Solicitors Regulation Authority (SRA number – 619586).

We pride ourselves on providing a quality service that delivers results which leaves our clients satisfied. With specialist solicitors who are leaders in their field, we're able to support people with cases relating to personal injury, medical negligence, data breach law and criminal injuries.

We believe everyone who has suffered harm, be it physically, psychologically or financially, should have access to justice and quality representation to help restore balance back in their lives, help them achieve justice for the wrongs they've suffered, and to help them recover compensation to account for their losses and suffering.

The vast majority of our cases are run under No Win No Fee agreements, meaning you can begin a claim without having to worry about the costs of funding the action.

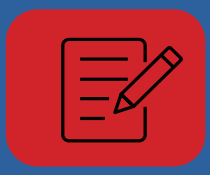
GET IN TOUCH

Our team of advisers are on hand 24 hours a day, 7 days per week to offer you the help and support you need. You can speak with us today by:

Calling 0800 073 8804

Chatting with us now via our live chat on www.legalexpert.co.uk

Or by writing to us via the contact form on our website.




POLICE
POLICE