28 August 2025

APCS Data Breach | FAQs

About the breach

What has happened?
We have been notified that one of their suppliers Access Personal Checking Services Ltd (APCS) has been subject to a significant data breach. ACPS carries out Data and Barring Services (DBS) checks on behalf of the National Church Institutions (NCIs), some Dioceses and Parochial Church Council (PCCs). The breach has affected clergy, lay ministers, volunteers, and staff.

Who has it affected?
This breach has impacted people across the Church who have been subject to a recent DBS check. APCS carries out DBS checks on behalf of some Dioceses and PCCs, and the NCIs.

Who are APCS and what do they do?
APCS specialise in processing disclosures for individuals and small business owners, large public and private sector companies, organisations, and recruitment agencies.

When did this happen?
APCS have stated that their external software supplier, Intradev, notified them on 17 August that their system had been compromised between the 31 July 2025 and 15 August 2025, and certain files containing personal details were copied. APCS were provided with copies of the compromised data on Monday 18 August. APCS' own network and servers were not compromised. From initial assessments made by APCS, the data that is affected is from 1 December 2024 to 9 May 2025.

Have other organisations outside of the C of E been affected?
Yes. APCS provides Data and Barring Services (DBS) to many organisations. This breach also impacts those bodies.

How confident are we that only those notified have been affected?
APCS have started the process of notifying those individuals affected by the breach. APCS have said that the breach only affects those individuals who were subject to a DBS check between the 1 December 2024 to 9 May 2025, but this is a moving situation, and we will keep you updated as we receive more information.

Is this data breach connected to the data incident involving the independent Redress Scheme?
No. The two incidents are unconnected.

What personal information has been leaked?
We are waiting for more details from APCS. We understand that the breach may have affected some or all the following information:

- Name, phone number, date of birth, email address, address, place of birth, National Insurance number, passport number, driving licence number.

It does not include:

- Medical information, information on any disclosures, information about your protected characteristics e.g., ethnicity, disability, sexual orientation, marital status.

The information that was accessed was in text format only. No documents, images, passwords, or financial details were affected.

What are the Hereford Diocese doing?
Although this breach has been caused by APCS and their Intradev system, it is the Diocesan staff in the office who are doing all of the contacting and sorting out of this issue. So far:

- People affected by the data breach have been contacted with advice and support.
- Support includes 12 months free access to a credit checking and monitoring service from Experian.
- Bishop Richard has contacted people personally affected
- All DBS checks with APCS have been paused until further notice.
- Webpages have been created and Parish Safeguarding teams have been contacted.
- This incident has been reported to the Information Commissioner's Office (ICO) and the Charity Commission.

Reporting the breach and data protection

Do PCCs need to report the incident to the ICO?
Yes. PCCs should report separately to the ICO if they have directly accessed the service i.e. if they have been uploading data to APCS themselves this makes them the data controller. If the DBF have been doing this on their behalf, then the DBF should report as the data controller. You can assess this by checking who APCS is corresponding with i.e. if they have contacted the PCC directly, then it is likely that the PCC is the controller and therefore must report.

Whether the PCC is part of the national deal is not the issue for reporting to the ICO, the key issue is who the controller is, so if the PCC have their own contract with APCS and have been contacted, they must report it.

Who is responsible for reporting a breach to the ICO?
Only the data controller is responsible for reporting a high-risk data breach to the ICO. A high-risk data breach is one which has a significant effect on the rights and freedoms of data subjects. All parties are accountable for taking steps to mitigate the effects of the breach where possible.

If the data breach is caused by the processor, the processor must implement technical and organisational measures to assist the controller to deal with the breach but is responsible for their own failures or those of their sub-processors. However, the ICO can investigate all parties involved to ensure they have met their obligations appropriately.

Do we need to report this incident to the Charity Commission?
The Charity Commission have informed the National Church Institutions that due to the large number of Serious Incident Reports they have received on this, trustees in PCCs and diocesan boards of finance do not need to report to the Charity Commission "if in substance they simply wish to report the same incident in materially similar terms".

Is the 72-hour deadline for reporting the incident to the ICO based on when an email notifying the breach was sent, or when the email was seen?
The 72-hour window is based on when your organisation became aware of the data breach (i.e. when the email sent from APCS was seen). If you have missed the 72-hour deadline, you can explain that the reason for the delay is because you were fact finding, but it is best if you can do this as close to the 72-hour window as possible.

I would like to request that any data held by APCS on me is deleted under GDPR. How do I go about this?
If you wish to make an erasure request, you can contact APCS via email to enquiries@accesspcs.co.uk or by phone on 0845 6431145. The APCS Privacy policy is available here: www.onlinecrbcheck.co.uk/docs/privacypolicy.pdf

What's the difference between a data controller and a data processor?
A **data controller** is the organisation responsible for making the key decisions about how and why data is collected, stored, and used and is responsible for complying with all GDPR obligations. Where the controller uses an external supplier who will be processing personal data for the controller (data processor), the overall responsibly for data protection compliance remains with the data controller.

A controller is responsible for ensuring that the processors have provided sufficient assurance that they are GDPR compliant, and for putting in place a suitable contract which should include instructions on how a data breach will be managed.

In the APCS situation the controller would be the organisation responsible for uploading data to the APCS system, for example the Church of England Central Services, a Diocesan Board of Finance, or Parochial Church Council.

A **data processor** is responsible for processing personal data solely on behalf of the controller adhering strictly to the controller's documented instructions. They are responsible for complying with their own GDPR obligations, including putting in place a suitable contract which provides an equivalent level of data protection as the contract with the controller. with any of their sub-processors

The processor must immediately inform the controller of any data breaches. In this case APCS is the data processor.

A **sub-processor** is a supplier providing processing services to the primary data processor. They are responsible for processing personal data on behalf of the primary data processor, under a suitable contract. This includes implementing appropriate security measures to protect the data, complying with relevant GDPR obligations and assisting the primary processor and controller to meet their data protection obligations. In this case Intradev is the sub processor.

Why are parishes being asked to submit a report to the ICO?
In the event of a data breach, the data controller is responsible for submitting a report to the ICO. In this instance, the "controller" is the organisation responsible for uploading data to the APCS system, for example, the PCC.

Support for people affected

What support is available for those who have been affected?
Access to a credit checking and monitoring service from Experian is being made available for 12 months for those affected. If you have been affected by this data breach and you have not received a code to access your Experian Identity Plus account, please contact k.preedy@hereford.anglican.org. More information about the service available from Experian is contained within these FAQs.

Advice about what additional steps you can take, and the resources available to help protect you from fraud, are also included in these FAQs.

Who can I contact about the data breach?
k.preedy@hereford.anglican.org

If my passport and driving licence details have been accessed, should I apply for new ones?
We do not believe it is necessary to replace driving licences or passports, as the images associated with these documents were not breached. However, if you feel strongly about this then we suggest that you keep a copy of any costs incurred so that we can seek compensation from APCS.

What support will I be offered if my data is used maliciously through this breach? For instance, if someone uses the data to create a new payment from my bank account or creates a credit agreement that negatively affects my credit file?
We are encouraging all colleagues who are potentially affected by this to sign up to the Experian service. This service, provided for 12 months, will help you to keep an eye out for any changes that suggest someone is using your data improperly – for instance, you will get an alert if someone sets up a new credit agreement. If you become the victim of fraud, you will be offered help through Experian's caseworker service to get back on track and sort out your credit file.

In addition, you should look out for any unwanted calls, emails or contact to you directly, including monitoring your bank account. You might find it helpful to talk to your bank now to let them know of the situation. Some are able to put in place additional identification verification checks for making/setting up payments, to help keep your money safe.

If I lose money or my credit file is affected due to fraud, will I be compensated?
The Diocese will work alongside you and do what we can to ensure no colleagues loses out as a result of this breach by APCS. In the hopefully rare event where someone suffers a loss, we will work with you to help rectify the situation.

What can I do to protect myself from fraud?

- Stay alert to unexpected emails, calls, or letters that mention personal details about you
- Never give personal information to unsolicited callers, even if they seem to know details about you
- Verify any unexpected contact by calling the organisation directly using their official number
- Monitor for new applications made in your name:
    - Check your credit report – see below for information about the service that will be available to you from Experian shortly.
    - Look for any new accounts, credit searches, or applications you did not make.
- Inform your bank, building society and credit card company of any unusual transactions on your statement.

Links and contact numbers

Action Fraud
The government has put together **this checklist to help on the steps to take to repair your identity** and prevent re-victimisation.

The National Fraud and Cyber Crime Reporting Centre has a wealth of advice and resources on the Action Fraud website.

- www.actionfraud.police.uk
- Call Action Fraud on 0300 123 2040

GOV.UK

- Advice from GOV.UK on the actions you should take if you have shared personal information

Financial Ombudsman Service

If you have lost money because of fraud or a scam – and you are unhappy with how your bank or payment service provider handled things – The Financial Ombudsman Service may be able to help.

- www.financial-ombudsman.org.uk/consumers/complaints-can-help/fraud-scams

General advice

- www.citizensadvice.org.uk
- Call Citizens Advice on 0808 223 1133

To report the theft or loss of post

- Royal Mail website: www.royalmail.com/report-a-crime
- Or call Royal Mail on 08457 740 740

Experian Identity Plus

Who can I speak to about getting an access code for the credit check and web monitoring service from Experian?

k.preedy@hereford.anglican.org

What does the Experian Identity Plus account provide?

Features of the Experian Identity Plus account includes:

- **Daily Experian Fraud Report**
  If you log in, you can get your daily Experian Fraud Report. This details key information from your Experian Credit Report that may help you identify fraudulent activity on your credit report.
- **Alerts provided as part of the service**
  Alerts will be provided by email and/or SMS, depending on your settings and features availability.
- **Experian fraud alerts**
  Get alerts by email and/or text message about certain changes to your Experian Fraud Report. Alerts relate to when accounts are opened or closed, or when your credit report is searched. Some of our credit alerts may be sent in real-time to notify of certain changes when they happen, others are sent weekly.
- **Experian CreditLock alerts**
  Experian will let you know when your Experian credit file is searched and if your credit file was locked. For any applications that are blocked you will be sent a message by email and/or text to make you aware.
- **CreditLock**
  Experian CreditLock is designed to reduce fraudulent credit applications. Locking your Experian Credit Report will help to block new fraudulent credit applications made in your name, using your information from the Experian Credit Bureau.
- **Web monitoring**
  Experian will help you better protect your identity by scanning certain internet sites and

locations for selected personal and financial details and alerting you by email or text message if anything looks wrong or fraudulent. Alerts are sent every day that we find suspicious information. Web monitoring is designed to work alongside taking a cautious approach to your sharing of data and use of the internet and other digital services.

Read this guide to Identity Plus for more details

How do I read my credit report? I have never had one before
If you are not sure where to start, take a look at this guide from Experian: www.experian.co.uk/consumer/experian-credit-report.html

Your credit report has different sections. For instance, it will show information about you, any credit agreements you have (e.g. your mortgage or with a phone company), your financial connections (e.g. spouses/partners), and details of any missed/overdue payments on credit agreements.

What happens beyond 12 months with the Experian service?
At the end of the 12-month period the individuals will get an email to say their subscription is coming to an end and the options available to them.

How up to date is Experian? For instance, if someone set up a credit agreement today, would they tell me today?
Through your Experian Identity Plus subscription*, you will be offered daily alerts as to whether something has changed within your credit report. The subscription also allows you to lock your Experian credit report to help stop fraudsters taking out agreements in your name.

I have been advised to use CIFAS as well. Is this necessary?
Experian is a member of CIFAS (Credit Industry Fraud Avoidance System) and can access data related to confirmed fraud cases. CIFAS focuses on fraud prevention; Experian offers identity verification and fraud prevention.

I already have an Experian account, or I have used Experian in the past. What should I do?
If when you log into Experian using the code we have given you, and you are using your personal email address, you may be told that you already have an account under that username. In this case either continue to use your existing account if you are still paying for it and let us know that you do not need the code or create a new account using a different email address.

If you need further assistance, please call the Experian support line on 03444 818182.

Experian asks for a lot of personal data, should I be giving this to them
When you create the account, you will be asked for your email address as a username, you should use your own personal email account because reports from Experian contain your own personal financial information which should not be held in a work email inbox (see above).

You may be asked for date of birth and address so that Experian can identify you, and they may ask you for additional data, for example, your mother's name as an additional security check.

They will already know some of your financial arrangements e.g. mortgage information and bank account details etc, or other financial arrangements where you have had to get a credit check, and they will ask you to confirm these.

They need these details to ensure that they monitor all your financial arrangements, however, they also collect data for marketing purposes.

You should read their Privacy Notice here: **Experian Consumer Privacy Policy**
To opt out of marketing click here: **Opt out by marketing channel and industry sector - Experian Consumer Information Portal**

Other / general

I have been approached by a journalist to ask me about the breach. What do I do?
Please do not offer any comment and refer them to our communications team communications@hereford.anglican.org