Year	Ref	Date Identified	Type of Breach (e.g. personal data, contributions, criminal activity, etc)	Description	Action Taken in Response to Breach	Possible Impact (Red/Amber/ Green)	Date Reported to Local Pension Board or Authority	Reported to Pensions Regulator or other statutory body (e.g. ICO)?	Reported to Data Protection Officer?	Details of any follow up actions taken/required or wider implications	Breach Open/Closed
2020/21	51	29/03/21	Payment to wrong member	Individual with same name and date of birth as our scheme member claimed payment of deferred benefits.	Overpayment being recovered	Green	15/07/2021 (LPB)	NO	NO	Correct member identified for payment of benefits.	Open pending any Board comments
2021/22	53	06/05/21	Personal Data	Member sent a P60 for themselves and a different member.	Apology issued and P60 destroyed	Green	15/07/2021 (LPB)	NO	NO	Printers carried out internal investigation and reported back.	Open pending any Board comments
2021/22	54	30/06/21	Personal Data	Wrong death certificate returned to NOK.	Apology issued and death certificate returned.	Green	15/07/2021 (LPB)	NO	NO	Check introduced to process to avoid future recurrence	Open pending any Board comments

Year	Ref	Date Identified	Description of Cybersecurity Incident	Action Taken in Response to Incident	Date Reported to Local Pension Board or Authority	Reported to Pensions Regulator or other statutory body (e.g. ICO)?	Reported to Data Protection Officer?	Details of any follow up actions taken/required or wider implications	Incident Open/Closed
2021/22	CS6	06/05/21	Phishing Email received from ampf to member of investment team.	All users informed of phishing email. The URL in the attachment was also blocked.	15/07/2021 (LPB)	NO	NO	Phishing email testing is planned as part of IT work programme to check users remain vigilant.	Closed
2021/22	CS7	13/05/21	Email sent to an employer purporting to be from a member of our team.	All employers notified to be aware of email.	15/07/2021 (LPB)	NO	NO		Closed
2021/22	CS8	18/06/21	Active Directory account locked out for staff member. Troubleshooting revealed the attempts were from an external source via the Mimecast service.	Default authentication profile modified to only allow access from SYPA owned IP addresses.	15/07/2021 (LPB)	NO	NO	Mimecast account lockout thresholds reduced to 3 failed attempts.	Closed
2021/22	CS9	01/07/21	Phishing Email received purporting to be from CEM Benchmarking.	All users informed of phishing email. The URL in the attachment was also blocked. Checked for other recipients reciving email.	15/07/2021 (LPB)	NO	NO	Phishing email testing is planned as part of IT work programme to check users remain vigilant.	Closed