Kamiah Jt. School District No. 304
1102 Hill Street, Kamiah, ID 83536
Phone: (208) 935-2991 Fax: (208) 935-4005

Paul Anselmo
Superintendent
(208) 935-4001
panselmo@kamiah.org

Sarah Cain
Business Manager
(208) 935-4004
scain@kamiah.org

Tracy Lynde
District Clerk/Treasurer
Human Resources Director
(208) 935-4003
tlynde@kamiah.org

January 10, 2025

Attorney General's Office Consumer Protection Division
P.O. Box 83720
Boise, ID 83720-0010

Re: PowerSchool Cybersecurity Incident

Dear Office of the Attorney General:

I am writing to notify you that Kamiah Joint School District 304 has experienced a data breach that resulted in some student and teacher personal information from our student information system (SIS) being compromised. On Tuesday, January 7th, our IT department was notified by PowerSchool, our SIS provider, "that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed." Following this notification, our IT staff reviewed data access logs and found that this party had accessed data from multiple tables in our SIS, the Student table and the Teacher table. The records contained in these tables are included as Appendix A.

On Wednesday, January 8th, we received a more in depth briefing from PowerSchool cyber security officials. In that briefing, they confirmed that only data from these tables had been taken from affected school districts across the country and globe. They further stated that they had engaged the firms CyberSteward and CrowdStrike to investigate and respond to the cybersecurity attack. That response included engaging with the party who breached their system and negotiating an agreement through which the party destroyed the stolen data.

On January 9th, we received further information from PowerSchool and templates for communication with parents and staff.

On the afternoon of January 10th, we notified our current employees and student families of the data breach by sending this statement to them via email, text message, and app notification, which is Appendix B. We have put Appendix B on the kamiahsd.org website under its own heading, PowerSchool Data Breach.

We have closed the back channel connection between our servers and the PowerSchool IT team and will only open that channel on an as needed basis for a limited amount of time. We are also reviewing other on-premise servers that house personal information to ensure other such connections are not kept open. At this time, based on the information and recommendations provided to us by the PowerSchool officials, we believe that there is no ongoing threat related to this security breach.

Thank you,

Paul Anselmo

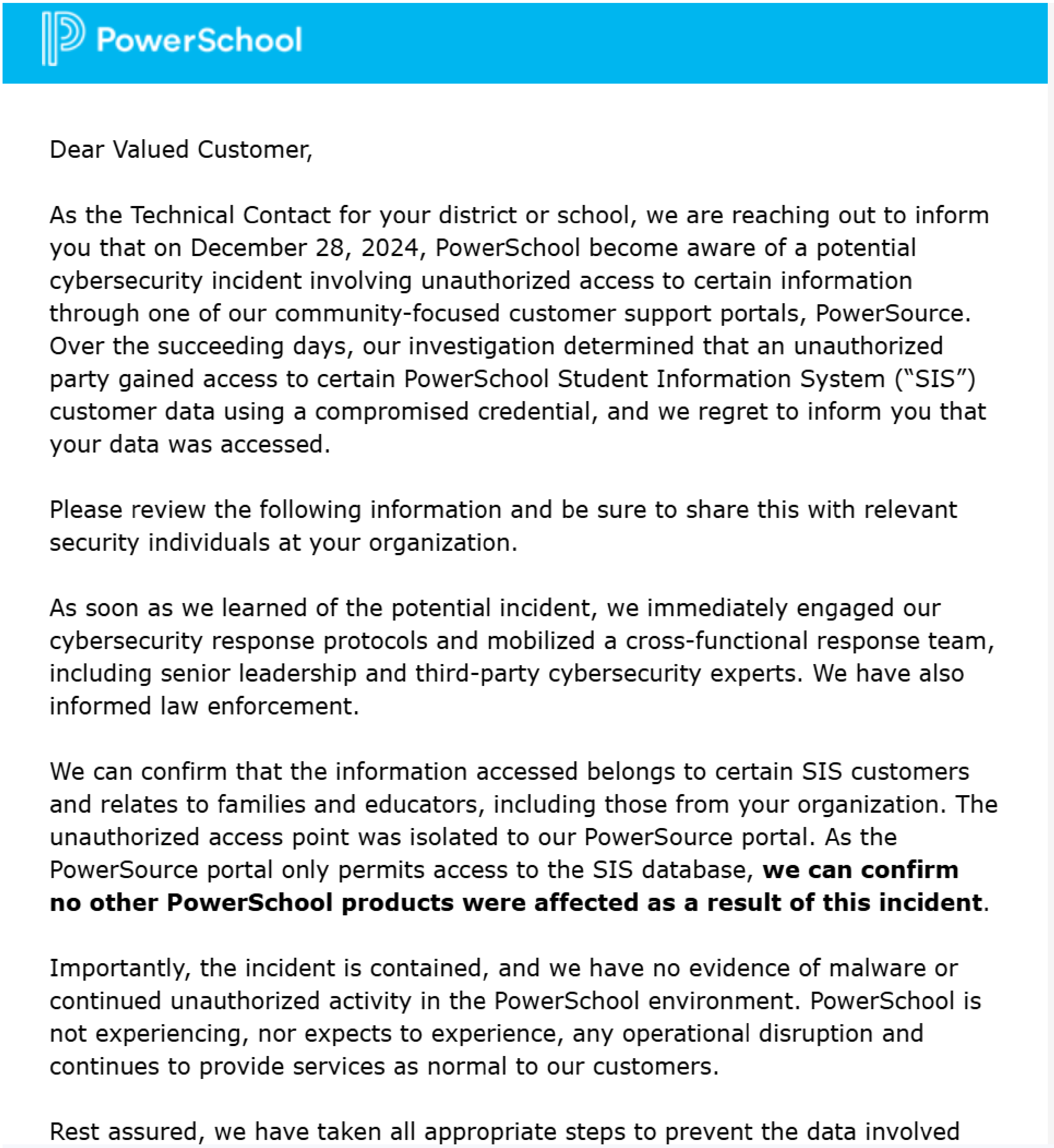
Appendix A:

Module: Students

Fields Exported: STUDENTS.Alert_Guardian, STUDENTS.Graduated_SchoolName, STUDENTS.State_ExcludeFromReporting, STUDENTS.Applic_Submitted_Date, STUDENTS.SDataRN, STUDENTS.Bus_Stop, STUDENTS.Student_AllowWebAccess, STUDENTS.LastMeal, STUDENTS.WHOMODIFIEDTYPE, STUDENTS.SchoolEntryDate, STUDENTS.WM_Address, STUDENTS.Mailing_City, STUDENTS.GPEntryYear, STUDENTS.Grade_Level, STUDENTS.Alert_OtherExpires, STUDENTS.TransferComment, STUDENTS.WHOMODIFIEDID, STUDENTS.Middle_Name, STUDENTS.CampusID, STUDENTS.Withdrawal_Reason_Code, STUDENTS.Next_School, STUDENTS.EnrollmentType, STUDENTS.Person_ID, STUDENTS.SummerSchoolID, STUDENTS.Team, STUDENTS.ExitDate, STUDENTS.City, STUDENTS.IP_ADDRESS, STUDENTS.Locker_Combination, STUDENTS.PhotoFlag, STUDENTS.Home_Phone, STUDENTS.Mailing_Street, STUDENTS.Student_Web_Password, STUDENTS.Ethnicity, STUDENTS.SchoolEntryGradeLevel, STUDENTS.Alert_Other, STUDENTS.WM_Password, STUDENTS.Doctor_Name, STUDENTS.StudentPict_guid, STUDENTS.Bus_Route, STUDENTS.FullTimeEquiv_obsolete, STUDENTS.House, STUDENTS.TuitionPayer, STUDENTS.Exclude_fr_rank, STUDENTS.TeacherGroupID, STUDENTS.Mailing_State, STUDENTS.StudentPers_guid, STUDENTS.SchoolID, STUDENTS.dcid, STUDENTS.DistrictEntryGradeLevel, STUDENTS.State_EnrollFlag, STUDENTS.WM_TA_Flag, STUDENTS.EntryCode, STUDENTS.Sched_NextYearGrade, STUDENTS.WM_Tier, STUDENTS.SummerSchoolNote, STUDENTS.WM_Status, STUDENTS.MembershipShare, STUDENTS.ExitCode, STUDENTS.GuardianFax, STUDENTS.Sched_NextYearTeam, STUDENTS.Track, STUDENTS.Sched_LoadLock, STUDENTS.GradReqSet, STUDENTS.Fee_Exemption_Status, STUDENTS.Cumulative_GPA, STUDENTS.Sched_Priority, STUDENTS.Locker_Number, STUDENTS.Alert_Discipline, STUDENTS.Alert_DisciplineExpires, STUDENTS.FedRaceDecline, STUDENTS.ID, STUDENTS.Sched_LockStudentSchedule, STUDENTS.WM_CreateTime, STUDENTS.Family_Ident, STUDENTS.Simple_GPA, STUDENTS.Sched_YearOfGraduation, STUDENTS.State, STUDENTS.Enrollment_Transfer_Info, STUDENTS.SSN, STUDENTS.Street, STUDENTS.Phone_ID, STUDENTS.PL_Language, STUDENTS.Enroll_Status, STUDENTS.Mailing_Geocode, STUDENTS.WM_TA_Date, STUDENTS.DistrictOfResidence, STUDENTS.DistrictEntryDate, STUDENTS.Enrollment_SchoolID, STUDENTS.Sched_Scheduled, STUDENTS.Zip, STUDENTS.StudentSchlEnrl_guid, STUDENTS.CustomRank_GPA, STUDENTS.EntryDate, STUDENTS.Sched_NextYearHouse, STUDENTS.Gender, STUDENTS.Student_Web_ID, STUDENTS.Sched_NextYearHomeRoom, STUDENTS.WM_CreateDate, STUDENTS.Lunch_ID, STUDENTS.LunchStatus, STUDENTS.Cumulative_Pct, STUDENTS.Father_StudentCont_guid, STUDENTS.Building, STUDENTS.Doctor_Phone, STUDENTS.ExitComment, STUDENTS.Web_ID, STUDENTS.Sched_NextYearBuilding, STUDENTS.State_StudentNumber, STUDENTS.Enrollment_Transfer_Date_Pend, STUDENTS.Geocode, STUDENTS.First_Name, STUDENTS.Graduated_SchoolID, STUDENTS.Simple_PCT, STUDENTS.GradReqSetID, STUDENTS.Guardian_StudentCont_guid, STUDENTS.Log, STUDENTS.DOB, STUDENTS.Last_Name, STUDENTS.WM_StatusDate, STUDENTS.Web_Password, STUDENTS.EnrollmentID, STUDENTS.Emerg_Phone_1, STUDENTS.Sched_NextYearBus, STUDENTS.Mother, STUDENTS.Emerg_Phone_2, STUDENTS.Alert_GuardianExpires, STUDENTS.Student_Number, STUDENTS.Home_Room, STUDENTS.ClassOf, STUDENTS.Balance1, STUDENTS.Alert_Medical, STUDENTS.Balance4, STUDENTS.Emerg_Contact_2, STUDENTS.Balance2, STUDENTS.Father, STUDENTS.Mailing_Zip, STUDENTS.Mother_StudentCont_guid, STUDENTS.Balance3, STUDENTS.LastFirst, STUDENTS.Applic_Response_Recvd_Date, STUDENTS.AllowWebAccess, STUDENTS.FedEthnicity, STUDENTS.LDAPEnabled, STUDENTS.FTEID, STUDENTS.EnrollmentCode, STUDENTS.GuardianEmail, STUDENTS.Alert_MedicalExpires, STUDENTS.Emerg_Contact_1, STUDENTS.Graduated_Rank, STUDENTS.TRANSACTION_DATE

Module: Teachers

Fields Exported: TEACHERS.Homeroom, TEACHERS.LoginID, TEACHERS.Sched_Lunch, TEACHERS.TeacherLoginID, TEACHERS.Zip, TEACHERS.TeacherNumber, TEACHERS.WM_Status, TEACHERS.ID, TEACHERS.StaffStatus, TEACHERS.NameAsImported, TEACHERS.WM_CreateDate, TEACHERS.AdminLDAPEnabled, TEACHERS.TeacherLoginPW, TEACHERS.Sched_TotalCourses, TEACHERS.WM_CreateTime, TEACHERS.SSN, TEACHERS.IPAddrRestrict, TEACHERS.State, TEACHERS.Home_Phone, TEACHERS.Sched_UseBuilding, TEACHERS.Classpua, TEACHERS.Sched_Team, TEACHERS.NoOfCurClasses, TEACHERS.Sched_MaxPreps, TEACHERS.WM_Address, TEACHERS.Email_Addr, TEACHERS.WM_StatusDate, TEACHERS.Sched_Scheduled, TEACHERS.Sched_IsTeacherFree, TEACHERS.Ethnicity, TEACHERS.TeacherLoginIP, TEACHERS.Access, TEACHERS.DefaultStudScrn, TEACHERS.StaffPers_guid, TEACHERS.AllowLoginStart, TEACHERS.PTAccess, TEACHERS.Sched_PrimarySchoolCode, TEACHERS.Sched_Substitute, TEACHERS.Sched_HouseCode, TEACHERS.Sched_Homeroom, TEACHERS.Sched_Classroom, TEACHERS.PowerGradePW, TEACHERS.Sched_MaxPers, TEACHERS.WM_TA_Flag, TEACHERS.PeriodsAvail, TEACHERS.HomePage, TEACHERS.Balance4, TEACHERS.Balance3, TEACHERS.Password, TEACHERS.Balance2, TEACHERS.Balance1, TEACHERS.Sched_ActivityStatusCode, TEACHERS.supportContact, TEACHERS.HomeSchoolId, TEACHERS.GradebookType, TEACHERS.NumLogins, TEACHERS.PreferredName, TEACHERS.Group, TEACHERS.AllowLoginEnd, TEACHERS.Sched_TeacherMoreOneSchool, TEACHERS.WM_Alias, TEACHERS.SchoolID, TEACHERS.TeacherLDAPEnabled, TEACHERS.CanChangeSchool, TEACHERS.Sched_MaximumDuty, TEACHERS.Sched_MaximumConsecutive, TEACHERS.LastFirst, TEACHERS.FedEthnicity, TEACHERS.City, TEACHERS.Notes, TEACHERS.WM_TA_Date, TEACHERS.PSAccess, TEACHERS.Photo, TEACHERS.Lunch_ID, TEACHERS.Maximum_Load, TEACHERS.Sched_Gender, TEACHERS.WM_Tier, TEACHERS.Sched_MaximumCourses, TEACHERS.Street, TEACHERS.WM_Exclude, TEACHERS.Middle_Name, TEACHERS.Users_DCID, TEACHERS.LastMeal, TEACHERS.Last_Name, TEACHERS.SIF_StatePrid, TEACHERS.FedRaceDecline, TEACHERS.WM_Password, TEACHERS.dcid, TEACHERS.Title, TEACHERS.Sched_MaximumFree, TEACHERS.Status, TEACHERS.First_Name, TEACHERS.Sched_Department, TEACHERS.Log, TEACHERS.Sched_BuildingCode, TEACHERS.School_Phone, TEACHERS.Sched_UseHouse



PowerSchool

Dear Valued Customer,

As the Technical Contact for your district or school, we are reaching out to inform you that on December 28, 2024, PowerSchool become aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed.

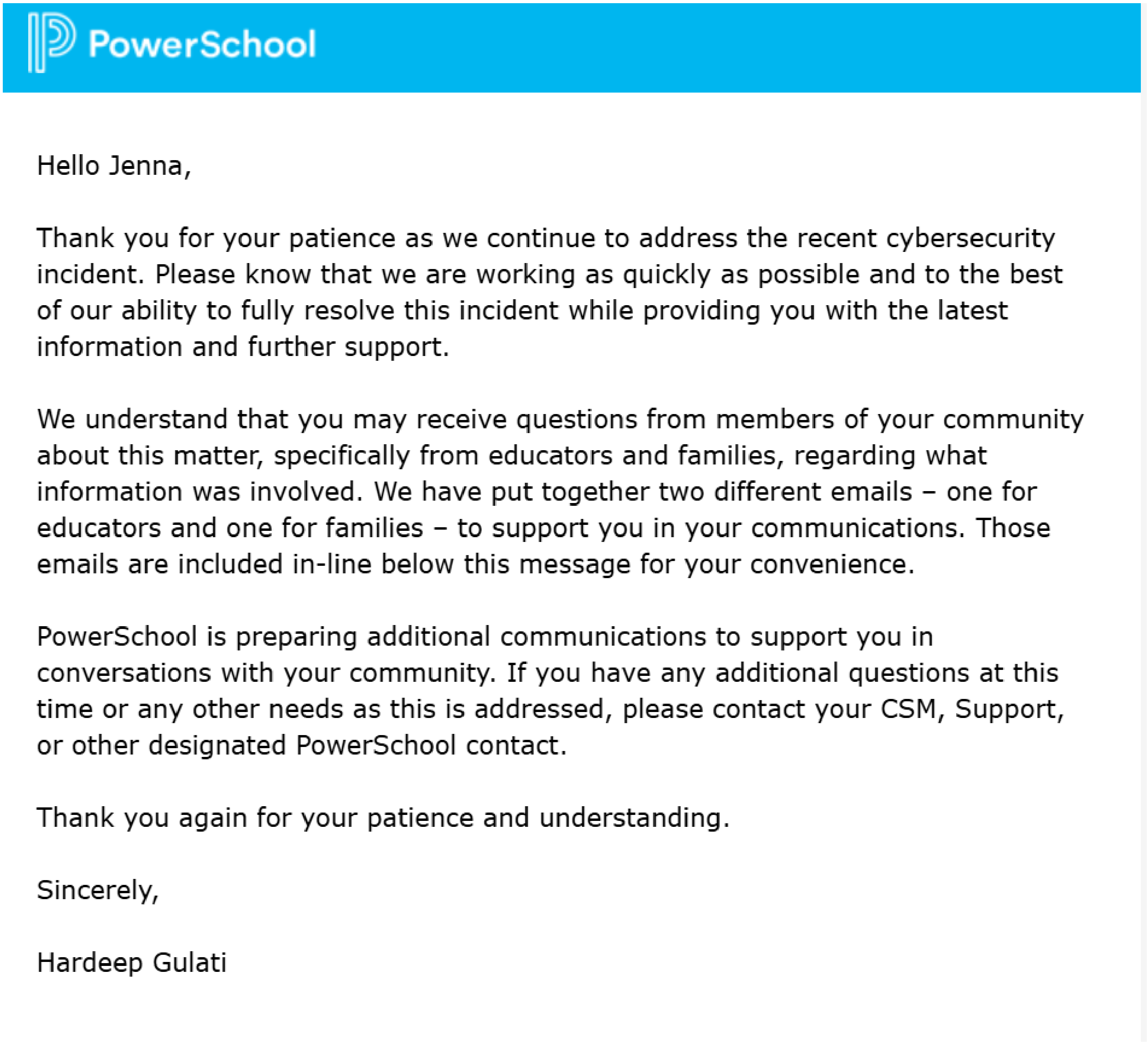
Please review the following information and be sure to share this with relevant security individuals at your organization.

As soon as we learned of the potential incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.

We can confirm that the information accessed belongs to certain SIS customers and relates to families and educators, including those from your organization. The unauthorized access point was isolated to our PowerSource portal. As the PowerSource portal only permits access to the SIS database, **we can confirm no other PowerSchool products were affected as a result of this incident**.

Importantly, the incident is contained, and we have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor expects to experience, any operational disruption and continues to provide services as normal to our customers.

Rest assured, we have taken all appropriate steps to prevent the data involved



PowerSchool

Hello Jenna,

Thank you for your patience as we continue to address the recent cybersecurity incident. Please know that we are working as quickly as possible and to the best of our ability to fully resolve this incident while providing you with the latest information and further support.

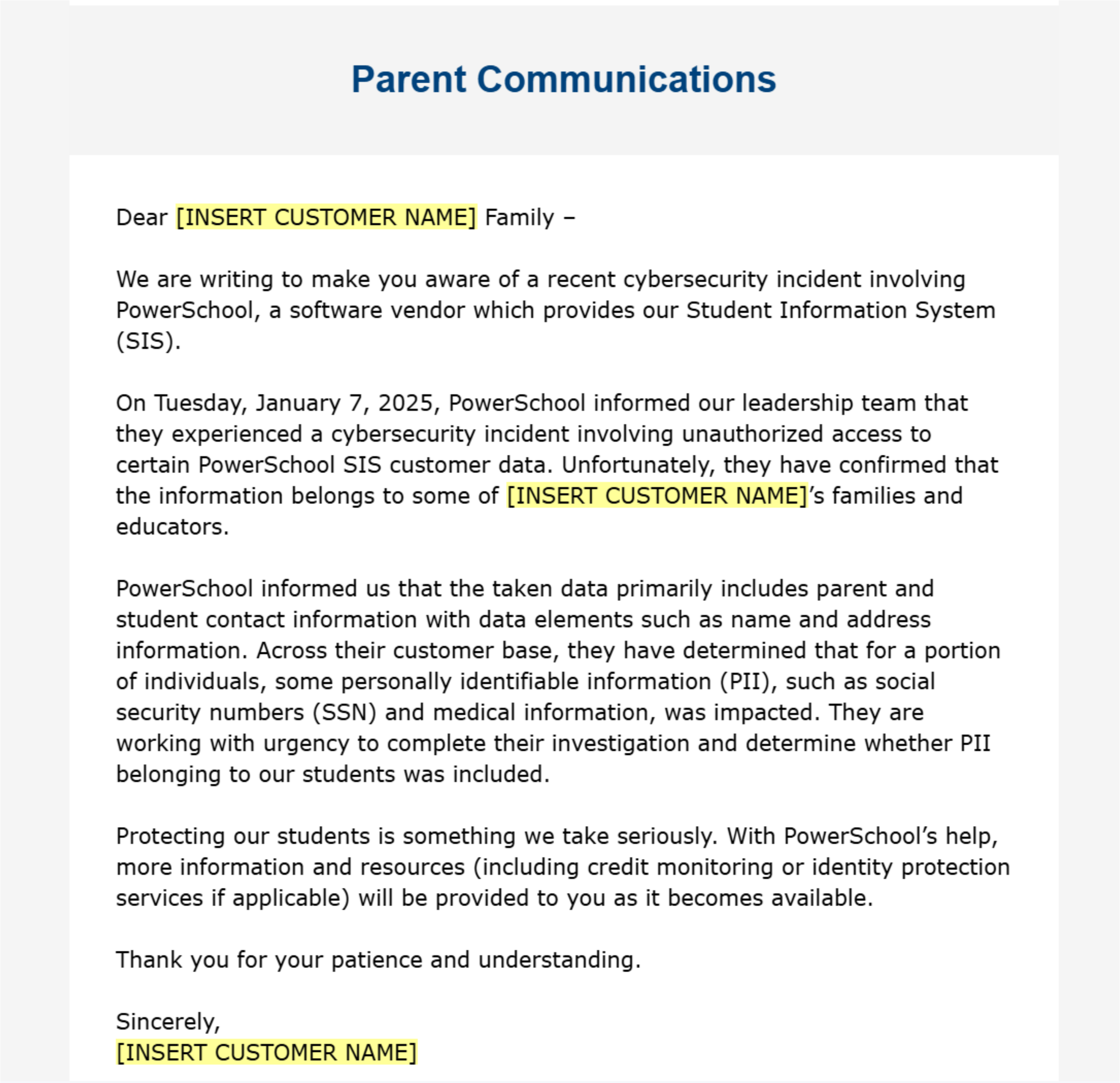
We understand that you may receive questions from members of your community about this matter, specifically from educators and families, regarding what information was involved. We have put together two different emails – one for educators and one for families – to support you in your communications. Those emails are included in-line below this message for your convenience.

PowerSchool is preparing additional communications to support you in conversations with your community. If you have any additional questions at this time or any other needs as this is addressed, please contact your CSM, Support, or other designated PowerSchool contact.

Thank you again for your patience and understanding.

Sincerely,

Hardeep Gulati



Parent Communications

Dear [INSERT CUSTOMER NAME] Family –

We are writing to make you aware of a recent cybersecurity incident involving PowerSchool, a software vendor which provides our Student Information System (SIS).

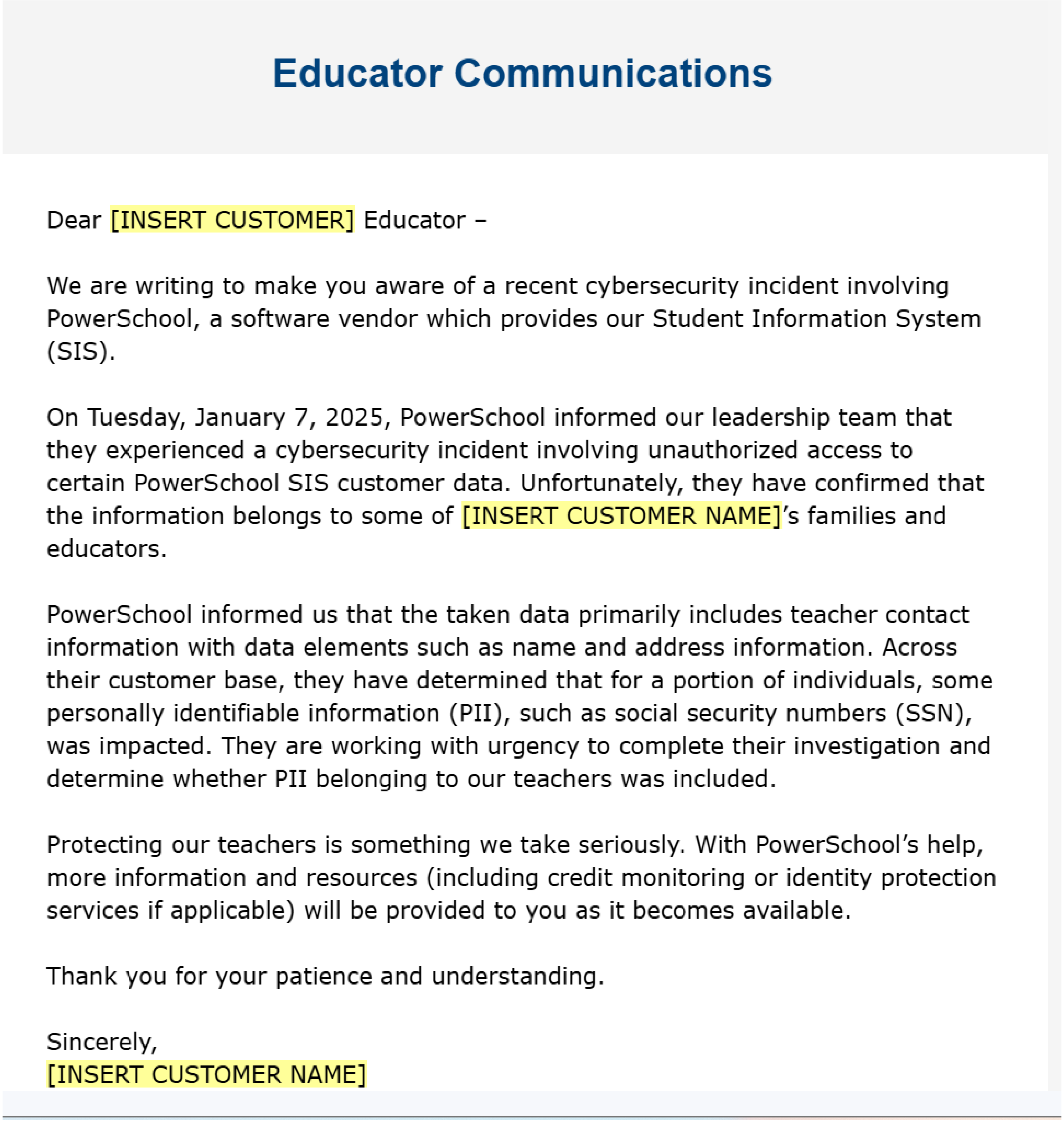
On Tuesday, January 7, 2025, PowerSchool informed our leadership team that they experienced a cybersecurity incident involving unauthorized access to certain PowerSchool SIS customer data. Unfortunately, they have confirmed that the information belongs to some of [INSERT CUSTOMER NAME]'s families and educators.

PowerSchool informed us that the taken data primarily includes parent and student contact information with data elements such as name and address information. Across their customer base, they have determined that for a portion of individuals, some personally identifiable information (PII), such as social security numbers (SSN) and medical information, was impacted. They are working with urgency to complete their investigation and determine whether PII belonging to our students was included.

Protecting our students is something we take seriously. With PowerSchool's help, more information and resources (including credit monitoring or identity protection services if applicable) will be provided to you as it becomes available.

Thank you for your patience and understanding.

Sincerely,
[INSERT CUSTOMER NAME]



Educator Communications

Dear [INSERT CUSTOMER] Educator –

We are writing to make you aware of a recent cybersecurity incident involving PowerSchool, a software vendor which provides our Student Information System (SIS).

On Tuesday, January 7, 2025, PowerSchool informed our leadership team that they experienced a cybersecurity incident involving unauthorized access to certain PowerSchool SIS customer data. Unfortunately, they have confirmed that the information belongs to some of [INSERT CUSTOMER NAME]'s families and educators.

PowerSchool informed us that the taken data primarily includes teacher contact information with data elements such as name and address information. Across their customer base, they have determined that for a portion of individuals, some personally identifiable information (PII), such as social security numbers (SSN), was impacted. They are working with urgency to complete their investigation and determine whether PII belonging to our teachers was included.

Protecting our teachers is something we take seriously. With PowerSchool's help, more information and resources (including credit monitoring or identity protection services if applicable) will be provided to you as it becomes available.

Thank you for your patience and understanding.

Sincerely,
[INSERT CUSTOMER NAME]

Appendix B

Kamiah Jt. School District No. 304

1102 Hill Street, Kamiah, ID 83536
Phone: (208) 935-2991 Fax: (208) 935-4005

Paul Anselmo
Superintendent
(208) 935-4001
panselmo@kamiah.org

Sarah Cain
Business Manager
(208) 935-4004
scain@kamiah.org

Tracy Lynde
District Clerk/Treasurer
Human Resources Director
(208) 935-4003
tlynde@kamiah.org

January 10, 2025

Kamiah Joint School District Students, Families, and Staff:

We share the same PowerSchool student information system as the majority of Idaho school districts. On January 7, 2025, PowerSchool notified our Leadership team that they experienced a cybersecurity incident involving unauthorized access to certain PowerSchool SIS data. On January 9, 2025, we received further communication from PowerSchool. Kamiah was among those notified as affected in the unauthorized data disclosure. We are required to notify individuals, students and families in a timely manner.

PowerSchool is working on assessing the depth of the breach with individual subscribers. We will keep our families updated should concerns with this cybersecurity incident arise.

Never hesitate to contact me with questions. I welcome the opportunity to discuss this further at 208-935-2991.

Thank you,

Paul Anselmo

Paul Anselmo

Superintendent, Kamiah Joint School District #304