Pointe Coupee Parish School Board
Post Office Drawer 579 • New Roads, Louisiana 70760-0579
(225) 638-8674 • Fax (225) 638-3237

November 10, 2025
VIA ELECTRONIC MAIL

UNDISCLOSED LOUISIANA DISTRIBUTION LIST

Re: Potential Cyber Incident

To Whom it May Concern:

On May 16, 2025, the Pointe Coupee Parish School Board ("School Board") began experiencing difficulty accessing certain portions of its local system. The School Board immediately contacted law enforcement and technology professionals to investigate the matter. Law enforcement and state officials subsequently confirmed that bad actors had accessed certain portions of the School Board's network, and therefore had the potential to exfiltrate data from the network (the "Incident'). The School Board was able to successfully remediate the vulnerabilities within its network, while continuing to provide basic services for its students.

The School Board has worked diligently to determine the types of data that may have been accessed by bad actors during the Incident. Although the School Board has no evidence that any of its data was ever acquired, out of an abundance of caution, the School Board believes it is possible the following types of data may have been stored on the system: first and last names of employees/students, social security numbers, driver's license numbers. The School Board is continuing to investigate and monitor the matter.

The School Board takes the security of its data very seriously. Accordingly, the School Board seeks to mitigate any potential risks by contacting those potentially impacted individuals with recommended response actions while the incident is investigated. Please read this letter and consider its contents carefully.

To best protect yourself from identify theft or any unintended consequences from the cyber incident, the School Board ***strongly encourages*** you to undertake the precautionary measures listed below for yourself and any members of your household:

1. Contact Equifax, Transunion, and Experian to request copies of your credit report, review the report for any suspicious activity, and request an active fraud alert. Also, the School Board strongly recommends obtaining a free security freeze with the following credit reporting agencies via telephone or at these websites:

Experian	**Equifax**	**Transunion**
(888)-EXPERIAN	(866) 885-2573	(800) 916-8800
(888-397-3742)	www.equifax.com	www.transunion.com
www.experian.com		

2. Change all passwords (and usernames if possible) for all accounts (such as banking, social media, secure portals, email, electronic health records, and cloud data storage), since certain online portals use personal identifying information to reset passwords. Any future passwords should be different and composed of a minimum combination of 9-12 random symbols and alphanumeric characters. If offered, each account should have multi-factor authentication enabled. Learn more about password protection at www.CISA.gov.

3. If you see any unauthorized activity on your credit report, promptly undertake the following actions:

    a. If you suspect any abnormal activity involving your data, including financial information, contact the Federal Trade Commission at 1-877-FTC-HELP or visit www.ReportFraud.FTC.gov immediately. Please also consider the following proactive measures:

    b. Contact the financial institution reporting abnormal activity and advise it that any such activity was fraudulently conducted without your consent.

    c. File a police report with your local law enforcement agency.

    d. File a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3") at www.ic3.gov.

    e. Complete and submit a Form 14039 Identity Theft Affidavit with the Department of the Treasury, Internal Revenue Service (found online here: https://www.irs.gov/pub/irs-pdf/f14039.pdf).

    f. Report fraud to the Social Security Administration through the Office of the Inspector General at 1-800-269-0271 or submit a report online at https://oig.ssa.gov/.

    g. Review signs of a scam online at https://www.ssa.gov/scam/.

4. If no abnormal activity was found on your credit report, still proceed with requesting an Identity Pin from the Internal Revenue Service for 2024 by signing up at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. The identity pin is a six-digit number randomly assigned to participants that prevents another individual from using your social security number to file tax returns on your behalf.

5. Continue to monitor your credit report regularly and consider registering for a ssa.gov myaccount at: https://secure.ssa.gov/RIL/SiView.action to prevent another individual from seeking social security benefits on your behalf (if eligible). Please note that you may need to wait to institute a fraud alert on your credit report if you wish to register for a ssa.gov myaccount.

6. Many cyber criminals use stolen personal identifying information to apply for government benefits. Therefore, and provided that you are not legitimately seeking benefits from these same agencies, please consider contacting the following government agencies and advising them not to accept fraudulent applications for benefits on your behalf:

a. The Small Business Association ("SBA"): SBA fraud may be reported via email at disastercustomerservice@sba.gov or through the Office of the Inspector General via written correspondence at 409 3rd Street, SW, Suite 7150, Washington, DC 20416.

b. The Federal Emergency Management Agency ("FEMA"): FEMA may be contacted at StopFEMAFraud@fema.dhs.gov or 1-866-720-5721.

c. The Louisiana Workforce Commission at www.Laworks.net and other state Unemployment Benefits Offices — a list of which may be found through the Department of Labor at: https://www.dol.gov/general/topic/unemployment-insurance.

Cybersecurity incidents impacting personal identifying information are becoming more frequent in modern society. Therefore, and even if no unusual activity was found on your credit report, please continue to monitor your credit report regularly.

Please feel free to contact the School Board with any questions at 225-638-8674. The School Board may be in touch, with further information, at a later date.

Very Respectfully,

Kim Canezaro

Kim Canezaro
Superintendent