Joseph M. Fusz
312.821.6141 (direct)
joseph.fusz@wilsonelser.com

February 23, 2026

Via Online Portal:

Attorney General Aaron Frey
Office of the Attorney General
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Notice of Cybersecurity Incident Involving Fort Scott Community College

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Fort Scott Community College ("FSCC"). The purpose of this correspondence is to provide your office with notice of a cybersecurity incident that was first discovered by FSCC on November 23, 2025, (hereinafter, the "Incident"). FSCC takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maine residents being notified, and the steps that FSCC has taken in response to the Incident. We have also attached a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring and identity theft protection services.

1. Nature of the Incident

On November 23, 2025, FSCC became aware of suspicious activity on its computer systems. FSCC immediately isolated the impacted systems and worked with its IT professionals and outside experts to secure and remediate these systems. FSCC engaged a third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The investigation revealed that data stored on the impacted systems may have been compromised and subject to unauthorized access. Based on these findings, FSCC conducted an extensive review of the impacted data files to identify the specific individuals and the types of information that may have been compromised. On January 30, 2026, FSCC finalized the list of individuals to notify.

2. Nature of Information Impacted

The type of information that may have been compromised include: Social Security Number, Financial Account Information, and Name. At this time, FSCC is not aware of any misuse of anyone's personal information and has not received any reports of fraud or identity theft related to this Incident.

3. Number of Maine residents affected.

A total of one (1) Maine resident may have been potentially affected by this Incident. The notification letter to this individual was mailed on February 23, 2026 by Certified Mail; Return Receipt Requested. A sample (redacted) copy of the notification letter is included with this letter as **Exhibit A**.

4. Steps taken in response to the Incident.

Data privacy and security is among one of FSCC's highest priorities, and FSCC is committed to doing everything it can to protect the privacy and security of the personal information in its care. Since the discovery of the Incident, FSCC immediately isolated the impacted systems and worked with our IT professionals and outside experts to secure and remediate these systems. FSCC engaged a third-party cybersecurity firm to conduct a comprehensive forensic investigation to determine the nature and scope of the Incident. They are also implementing additional technical safeguards, enhanced security measures, and updated procedures to mitigate against the risk of future issues.

FSCC has also offered all impacted individuals with complimentary credit monitoring and identity theft protection services by Kroll for a period of twelve (12) months. In addition, FSCC has highlighted steps that individuals can take to protect themselves including actively monitoring their financial accounts and statements, requesting a free credit report, and placing a fraud alert or security freeze on their credit reports.

5. Contact information

FSCC remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at joseph.fusz@wilsonelser.com or 312-821-6141.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Joseph M. Fusz

327261663v.1

EXHIBIT A

327261663v.1

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

[redacted]

SCAN TO ENROLL

[redacted]

<<b2b_text_1 (Re: Notice of Data Security Event / Re: Notice of Data Security Breach)>>

Dear [redacted],

Fort Scott Community College ("FSCC") writes to inform you of a recent data security incident that may have impacted the security of your personal information. We are providing you with details about the event, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On November 23, 2025, we became aware of unauthorized activity within our network. Upon becoming aware of this activity, we immediately implemented our incident response plan and engaged a specialized third-party cybersecurity firm to investigate the nature and scope of the issue. This investigation found evidence that an unauthorized party accessed our network and may have accessed certain files within the network.

Based on the findings from the investigation, we diligently reviewed the potentially impacted files to identify and catalog the types of information present within them and any individuals to whom the information related. We completed our review and finalized the list of individuals to notify on January 28, 2026.

What Information Was Involved?

Based on the investigation, the following personal information relating to you was present within data potentially at risk: [redacted].

What We Are Doing.

Data privacy and security is among our highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since discovery of the incident, FSCC has moved quickly to respond, isolate, contain, and secure the impacted systems, and are implementing additional technical safeguards, enhanced security measures, and updated procedures to mitigate against the risk of future issues.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for [redacted] months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until [redacted] *to activate your identity monitoring services.*
Membership Number: [redacted]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction. We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

For More Information

If you have questions, please call 1-844-354-0038, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

We sincerely regret any concern or inconvenience this matter may cause, and remain dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Fort Scott Community College

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity. You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies. You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html

Equifax	P.O. Box 740241 Atlanta, GA 30374 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com/personal/credit-report-services
TransUnion	P.O. Box 1000 Chester, PA 19016 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

For Iowa and Oregon residents, you are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

For Massachusetts residents, you are advised of their right to obtain a police report in connection with this incident.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491. FSCC is located at 2108 South Horton Street, Fort Scott, KS 66701 and can be reached at 800-874-3722.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at www.ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/.

For Rhode Island residents, this data event involves 1 individual in Rhode Island. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.