**Sample Letter 1**

March 17, 2026

[Recipient Name]
[Recipient Address]
[City, State, ZIP]

**Notice of Data Security Incident**

Dear [Recipient Name]:

Thank you for being a customer of the Bank. Middlesex Federal Savings, F.A. ("Middlesex") is writing to inform you of a data security incident that may have involved your personal information. Please read this notice carefully to learn more about the incident and what you can do to protect yourself.

**What Happened**

On February 25, 2026, Middlesex became aware that an internal bank document, the Overdraft Aging Report dated February 24, 2026, was inadvertently emailed by a bank employee to an individual outside of Middlesex.

Upon learning of the incident, Middlesex immediately contacted the individual in receipt of the errant email and requested that they delete the email and confirm that no further distribution of the information had occurred. As a result of this outreach, the individual in receipt of the email confirmed they had deleted the email and that no further distribution had taken place.

At this time, there is no indication that your information has been further disseminated or was misused. Out of an abundance of caution, we recommend that you contact us to change your account number. Our retail team is ready and willing to assist you with this.

**What Information Was Involved**

The Overdraft Aging Report that was inadvertently disclosed contained the following categories of your personal and account information:

- Name
- Account number(s)
- Account balance(s)
- Account open and credit dates
- Overdraft status

**What We Are Doing**

Middlesex values your privacy and deeply regrets that this incident occurred. Upon discovering the incident, we acted promptly to contain it and have taken the following steps:

- **Contacted the unintended recipient:** Middlesex immediately reached out to the individual who received the email in error and requested deletion of the email and confirmation that no further distribution occurred.

- **Reviewed internal disclosures:** Middlesex confirmed with the employee involved that no additional unauthorized disclosures took place.
- **Reviewed our policies and procedures:** Middlesex is reviewing its internal procedures for handling and transmitting sensitive documents to help prevent a similar incident from occurring in the future and providing employees with additional training on data handling and email security. Middlesex maintains a written information security program designed to protect the personal information of its customers.

**What You Can Do**

We encourage you to remain vigilant by reviewing your account statements and credit reports for unauthorized activity. If you believe you may be the victim of identity theft, you should contact your local law enforcement representative, your state attorney general, and/or the Federal Trade Commission.

You have the right to obtain a police report if you believe you are the victim of identity theft or fraud. We encourage you to file a report with your local law enforcement agency if you notice any suspicious activity related to your information.

This incident has not been reported to law enforcement. Middlesex does not have any evidence of fraudulent use of the information involved in this incident as of the date of this notice.

**If you would like to have your account number changed**, please contact us directly at 617-666-4700 and a Middlesex representative will be happy to assist you.

Please also review the steps below (under "Steps You Can Take to Further Protect Your Information") for further information on protecting your personal information.

**For More Information**

If you have any questions about this incident, you can contact us at 617-666-4700 between 8:30 A.M. and 4:00 P.M. on Mondays through Fridays or 8:30 A.M. to 12:00 P.M. on Saturdays or email us at banklocal@middlesexfederal.com.

We regret any inconvenience this incident may have caused you. Middlesex takes the protection of your personal information very seriously and has taken steps to prevent a similar incident from occurring again.

Sincerely,

Christine J. Conrad
Senior Vice President – Operations & Innovation and Information Security Officer
Middlesex Federal Savings, F.A.
One College Avenue, Somerville, MA 02144
617-666-4700

**Sample Letter 2**

March 17, 2026

[Recipient Name]
[Recipient Address]
[City, State, ZIP]

**Notice of Data Security Incident**

Dear [Recipient Name]:

Thank you for being a customer of the Bank. Middlesex Federal Savings, F.A. ("Middlesex") is writing to inform you of a data security incident that may have involved your personal information. Please read this notice carefully to learn more about the incident and what you can do to protect yourself.

**What Happened**

On February 25, 2026, Middlesex became aware that an internal bank document, the New Overdraft Accounts Report dated February 24, 2026, was inadvertently emailed by a bank employee to an individual outside of Middlesex.

Upon learning of the incident, Middlesex immediately contacted the individual in receipt of the errant email and requested that they delete the email and confirm that no further distribution of the information had occurred. As a result of this outreach, the individual in receipt of the email confirmed they had deleted the email and that no further distribution had taken place.

At this time, there is no indication that your information has been further disseminated or was misused. Out of an abundance of caution, we recommend that you contact us to change your account number. Our retail team is ready and willing to assist you with this.

**What Information Was Involved**

The New Overdraft Accounts Report that was inadvertently disclosed contained the following categories of your personal and account information:

- Name
- Account number(s)
- Actual account balance(s) and average available account balance(s)
- Overdraft status

**What We Are Doing**

Middlesex values your privacy and deeply regrets that this incident occurred. Upon discovering the incident, we acted promptly to contain it and have taken the following steps:

- **Contacted the unintended recipient:** Middlesex immediately reached out to the individual who received the email in error and requested deletion of the email and confirmation that no further distribution occurred.

- **Reviewed internal disclosures:** Middlesex confirmed with the employee involved that no additional unauthorized disclosures took place.
- **Reviewed our policies and procedures:** Middlesex is reviewing its internal procedures for handling and transmitting sensitive documents to help prevent a similar incident from occurring in the future and providing employees with additional training on data handling and email security. Middlesex maintains a written information security program designed to protect the personal information of its customers.

**What You Can Do**

We encourage you to remain vigilant by reviewing your account statements and credit reports for unauthorized activity. If you believe you may be the victim of identity theft, you should contact your local law enforcement representative, your state attorney general, and/or the Federal Trade Commission.

You have the right to obtain a police report if you believe you are the victim of identity theft or fraud. We encourage you to file a report with your local law enforcement agency if you notice any suspicious activity related to your information.

This incident has not been reported to law enforcement. Middlesex does not have any evidence of fraudulent use of the information involved in this incident as of the date of this notice.

**If you would like to have your account number changed**, please contact us directly at 617-666-4700 and a Middlesex representative will be happy to assist you.

Please also review the steps below (under "Steps You Can Take to Further Protect Your Information") for further information on protecting your personal information.

**For More Information**

If you have any questions about this incident, you can contact us at 617-666-4700 between 8:30 A.M. and 4:00 P.M. on Mondays through Fridays or 8:30 A.M. to 12:00 P.M. on Saturdays or email us at banklocal@middlesexfederal.com.

We regret any inconvenience this incident may have caused you. Middlesex takes the protection of your personal information very seriously and has taken steps to prevent a similar incident from occurring again.

Sincerely,

Christine J. Conrad
Senior Vice President – Operations & Innovation and Information Security Officer
Middlesex Federal Savings, F.A.
One College Avenue, Somerville, MA 02144
617-666-4700

**Exhibit to Letters**

## Steps You Can Take to Further Protect Your Information

### Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

### Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the printable request form at https://www.annualcreditreport.com/manualRequestForm.action or fill out the online form at https://www.annualcreditreport.com/requestReport/requestForm.action. You may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

| | **Equifax** | **Experian** | **TransUnion** |
|---|---|---|---|
| **Contact Information** | (866) 349-5191<br>www.equifax.com<br>P.O. Box 740241<br>Atlanta, GA 30374 | (888) 397-3742<br>www.experian.com<br>P.O. Box 2002<br>Allen, TX 75013 | (800) 888-4213<br>www.transunion.com<br>2 Baldwin Place<br>P.O. Box 1000<br>Chester, PA 19016 |

### Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

## OTHER IMPORTANT INFORMATION

### Security Freeze

You have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

### Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://consumer.ftc.gov/identity-theft-and-online-security.

### Oregon Residents Only

You may contact the Oregon Department of Justice with questions or complaints related to this incident at: Oregon Department of Justice, Consumer Protection, 1162 Court Street NE, Salem, OR 97301; Toll-Free: 1-877-877-9392; Website: www.oregonconsumer.gov.