Brian Gill

From: Chief Brian Gill <bgill@ayer.ma.us>
Sent: Tuesday, November 25, 2025 6:43 PM
To: Robert Pontbriand
Cc: Carly Antonellis; Deputy Chief Jen Bigelow
Subject: Flock Safety Project Benefits

Categories: Munsen / Flock PRR

Mr. Pontbriand,

Good evening.

As you know, we are continually evaluating products to enhance the safety and security for those within the Town of Ayer. As such, I wanted to provide you with a brief overview of a recently awarded grant funded project that truly enhances the safety and security of the Town, Flock Safety.

Approximately one year ago, we began engaging with Flock Safety, a nationally recognized provider of automated license plate recognition (ALPR) and Pan-Tilt-Zoom (PTZ) camera technology. Their system captures time-stamped vehicle data from strategically identified locations, giving investigators reliable information that significantly speeds up their investigation. Flock technology has been successfully used locally and nationwide to solve homicides, missing persons cases, motor vehicle and property crimes, assaults and other high-profile investigations.

Because of growing budget uncertainty, we decided to table the project with the hopes of revisiting it through grant funding. Recently, we learned that we were being awarded such funding through a state grant.

Some of the key benefits to the Town:

1. **Improved Crime Prevention and Investigations**: Flocks ALPR system provided immediate, actionable investigative information by identifying vehicles associated with criminal activity, enabling faster case resolution and more efficient patrol deployment.
2. **Force Multiplier at No Additional Personnel Cost**: The technology provided 24/7 monitoring of key areas, enhancing situational awareness and investigative capability without increasing staffing needs.
3. **Enhanced Regional Collaboration**: Flock's platform allows for secure information sharing within the Commonwealth and among out neighboring jurisdictions who are deploying the same technology, strengthening investigative efforts across municipal boundaries.
4. **Valuable Traffic Analytics**: The technology provides data on traffic volume, flow patterns, and repeat vehicle activity, supporting roadway planning, enforcement strategies, and future grant applications.
5. **Responsible Use of LPR and PTZ Camera's with Strong Privacy Safeguards**: LPR units collect only vehicle data, not faces or biometrics, and PTZ cameras are utilize strictly for public safety purposes in areas with no expectation of privacy. All use of data is governed by policy, clear

retention schedules, access controls, and audit logs to ensure transparency and maintain community trust.

As always, I am always available to discuss and questions or concerns you may have.

Thank you for your continued support of this project.

Chief Brian Gill
Ayer Police Department

54 Park St
Ayer, Ma 01432
978-772-8200 ext 501
978-772-8202 (F)
bgill@ayer.ma.us

Brian Gill

From: Chief Brian Gill <bgill@ayer.ma.us>
Sent: Monday, November 17, 2025 5:14 PM
To: Robert Pontbriand
Cc: Carly Antonellis; Deputy Chief Jen Bigelow
Subject: Fw: Legal Advisory: ACLU Letter Regarding License Plate Readers
Attachments: ACLU of Massachusetts Letter to Municipal Leaders Regarding Flock Safety License Plate Reader Technology.pdf; Advisory (ACLU Letter Regarding LPRs) (11.17.2025).pdf

Categories: Munsen / Flock PRR

Mr. Pontbriand,

Good evening.

Today we received this legal advisory from the MA Chief's Attorney regarding a letter being sent to Municipal Leaders whose police departments utilize LPR devices, specifically Flock Safety platform. As you know, we have received state grant funding to initiate the usage of Flock Safety and are proceeding toward implementing a combination of LPR and Video devices to aid on-going investigations.

The ACLU's stated concern in the letter (attached) is that the information can be shared nationwide, used by other government entities for purposes not in line with that of the Commonwealth's.

This information came to me at a good time, because I was already scheduled for an implementation meeting with Flock Safety this afternoon. I was informed by the implementation team that we can absolutely adjust the settings to have Ayer information to be only automatically accessed by Police Departments within the Commonwealth, further describing other states have that provision in law. I informed the implementation team that I wanted the settings to be set up that way, so that only Police Departments within the Commonwealth can access the data to assist their investigations.

Please advise if you need any further information.

Respectfully,

Chief Brian Gill
Ayer Police Department

From: masschiefs@memberclicks-mail.net <masschiefs@memberclicks-mail.net> on behalf of legal@masschiefs.org <masschiefs@memberclicks-mail.net>
Sent: Monday, November 17, 2025 2:33 PM
To: Chief Brian Gill <bgill@ayer.ma.us>
Subject: Legal Advisory: ACLU Letter Regarding License Plate Readers

Legal Advisory: ACLU Letter Regarding License Plate Readers

Dear Chief,

Many of you have received a recent letter from the ACLU of Massachusetts regarding the use of Flock Safety and other vendor-hosted license plate reader systems. MCOPA has prepared the attached advisory to help you understand the issues raised, identify key legal considerations, and determine appropriate next steps in coordination with your municipal or campus counsel.

The advisory is educational and does not direct agencies to take any specific action. It summarizes the ACLU's assertions, highlights relevant legal and operational considerations for Massachusetts agencies, and outlines steps you may consider as you review your contracts, system settings, and policies.

Please share this information with your counsel, chief administrative officer, and any local officials involved in technology procurement or data governance.

Attachments:

- MCOPA Advisory: ACLU Letter Regarding License Plate Readers
- ACLU Letter to Municipal Leaders

Please let me know if you have any questions.

Best,
Eric

Eric R. Atstupenas, Esq.
General Counsel
Massachusetts Chiefs of Police Association, Inc.
353 Providence Road
South Grafton, Massachusetts 01560

Office: (508) 375-7793
Mobile: (508) 400-3726
legal@masschiefs.org

Connect with Us:

ACLU of Massachusetts
One Center Plaza, Suite 850
Boston, MA 02110
617-482-3170

www.aclum.org

Dear Municipal Leader,

If your police department uses Flock Safety's license plate reader technology, sensitive data about your residents may be automatically shared with thousands of law enforcement agencies nationwide, including those involved in civil immigration enforcement and in states that ban abortion. Moreover, this data sharing undermines the effectiveness of the Massachusetts Shield Law and potentially violates its protections.

If your police department uses Flock or a similar license plate reader (LPR) provider, we urge you to take immediate action to: (1) disable any nationwide data sharing features, and (2) amend contract language that may give the company the legal right to share your jurisdiction's data.[1]

We strongly recommend you take the following steps within the next 30 days:

1. **Inquire with your police department** to determine if they use Flock Safety or other LPR technology.
2. **Request documentation** from your police department showing current Flock or other LPR system settings and complete contract terms.
3. **If they do use Flock or another LPR provider, immediately instruct them to:**
    a. Disable all automated data sharing with agencies outside Massachusetts, and
    b. Review and amend any contract language to ensure it does not give the LPR company rights to share your municipality's data.
4. **If external data sharing cannot be prevented,** end your LPR contract and remove the cameras from your community.

If your local government has not contracted with Flock or another LPR provider, we urge you to work with your police department to exercise extreme caution if approached by representatives from the LPR industry.

What is Flock Safety?

Flock sells license plate readers and database software to police departments, federal agencies, and private corporations across the country. These cameras collect data indicating who is driving, where, and when—for every car that passes, not merely cars associated with suspected criminal activity. Flock stores this information in a proprietary database.

---

[1] Note that Flock Safety is not the only company that offers police a nationwide license plate reader database. Vigilant Solutions, owned by Motorola, offers a similar system. The concerns outlined in this letter apply to all LPR systems.

Data Sharing Options

Police departments that contract with Flock can choose from several data sharing settings, including:

- No sharing outside the department
- Sharing only with specific, named police departments
- Sharing only with Massachusetts police departments
- Sharing with all government customers nationwide

The Contract Language Problem

Even when departments select restrictive administrative settings, there's an additional concern. According to documents obtained by the ACLU through public records requests, Flock's standard contracts with Massachusetts police departments include language giving the company "a non-exclusive, worldwide, perpetual, royalty-free right and license [to] disclose the Agency Data (both inclusive of any Footage) to enable law enforcement monitoring against law enforcement hotlists as well as provide Footage search access to law enforcement for investigative purposes only."

This contract language may supersede your police department's selection of restrictive settings, meaning departments must amend their contracts with Flock to ensure their data is truly protected.

The Scope of the Problem

Public records recently obtained by the ACLU reveal that Flock Safety's nationwide information sharing network allows external federal, state, and local law enforcement to access sensitive license plate data from dozens of Massachusetts cities and towns without a warrant or meaningful oversight.

According to these records, police departments in Massachusetts are currently sharing data with thousands of departments nationwide. Records show that police in states like Florida and Texas have searched license plate reader data through the Flock nationwide database, including for explicit immigration enforcement purposes and at least one abortion-related investigation.[2] Police departments have also searched the nationwide database on behalf of the FBI, DHS, and Border Patrol.

Put simply: if your local police are sharing data with Flock's national database, police from thousands of outside jurisdictions can track Massachusetts residents—including immigrants, people seeking

---

[2] Jason Koebler and Joseph Cox, Had an Abortion for Her 'Safety.' Court Records Show They Considered Charging Her With a Crime, 404 Media (Oct. 7, 2025), https://www.404media.co/police-said-they-surveilled-woman-who-had-an-abortion-for-her-safety-court-records-show-they-considered-charging-her-with-a-crime/; Dave Maass and Rindala Alajaji, Flock Safety and Texas Sheriff Claimed License Plate Search Was for a Missing Person. It Was an Abortion Investigation, Electronic Frontier Foundation (Oct. 7, 2025), https://www.eff.org/deeplinks/2025/10/flock-safety-and-texas-sheriff-claimed-license-plate-search-was-missing-person-it.

reproductive or gender-affirming care, elected officials, and other targets of the federal government—as they drive through our communities.

Even worse, according to Senator Ron Wyden and Rep. Raja Krishnamoorthi, Flock's failure to require customers to use industry standard security measures to protect their accounts has led to serious cybersecurity breaches of Flock's data. In a letter calling on the FTC to investigate the company, the members of Congress pointed to at least 35 cases in which Flock passwords had been stolen, and evidence "from a Russian-language cybercrime forum in which Flock accounts appear to be offered for sale."[3]

Massachusetts Shield Law

The Massachusetts Shield Law was designed to help protect people from other states' laws that criminalize abortion and restrict access to gender-affirming care, ensuring that people who receive and provide protected healthcare that is lawful in Massachusetts can do so without fear of retribution from out-of-state actors.

The law is clear: officers and employees of Massachusetts law enforcement agencies may not "provide information or assistance to any federal law enforcement agency or any other state's law enforcement agency...in relation to an investigation or inquiry" into reproductive healthcare or gender-affirming healthcare that is lawful in the Commonwealth. *See* Section 63(b) of Chapter 147.

Why Flock's System Undermines Shield Law Compliance

Flock Network Audits shared by Massachusetts police departments make clear that the nature of Flock's nationwide database system threatens the very purpose of the Shield Law. Flock's system automates data sharing and does not require individualized reviews of investigations or search queries of Massachusetts-collected data.

Records obtained by journalists confirm that in at least one case, police in Texas searched Flock's database to try to track down a woman they suspected of self-managing an abortion.[4] Among the records searched in that case was data from Massachusetts. As this incident demonstrates, Massachusetts police department participation in nationwide LPR data sharing operations could inadvertently share the very information the Shield Law was intended to protect.

---

[3] Letter from Senator Ron Wyden and Representative Raja Krishnamoorthi, to Federal Trade Commission Chair Andrew N. Ferguson (Nov. 3, 2025), https://www.documentcloud.org/documents/26212269-wyden-flock-ftc-letter/.
[4] Jason Koebler and Joseph Cox, Police Said They Surveilled Woman Who Had an Abortion for Her 'Safety.' Court Records Show They Considered Charging Her With a Crime, 404 Media (Oct. 7, 2025), https://www.404media.co/police-said-they-surveilled-woman-who-had-an-abortion-for-her-safety-court-records-show-they-considered-charging-her-with-a-crime/.

Flock Data and Mass Deportations

The Shield Law is not the only reason to stop sharing data with Flock's nationwide system. By sharing LPR data with a nationwide network of police departments and federal agencies, Massachusetts law enforcement also risks inadvertently providing information to out-of-state police that could contribute to serious human and civil rights violations.

The Florida Highway Patrol Example

The Florida Highway Patrol has been deputized to perform federal immigration enforcement and frequently queries the Flock national database. According to records obtained by the ACLU of Massachusetts, the Florida Highway Patrol searched the Flock nationwide database over 12,000 times from the start of 2025 through the end of July, including for explicitly stated immigration-related reasons.

Because Florida law requires police to engage in civil immigration enforcement,[5] it is likely that Florida's use of Flock data is directly feeding that state's immigration enforcement efforts. This potentially includes the arrest and detention of people at "Alligator Alcatraz," the state's detention camp for immigrants. Conditions there are appalling, with detainees facing unsafe climate conditions, inedible food, inadequate medical care, and extreme overcrowding.[6] In late September 2025, immigration attorneys sounded the alarm about a new low: as many as two-thirds of the people detained there had disappeared from ICE's detainee tracking system, leading advocates to call the detention center an "extrajudicial black site."[7]

Communities that seek to protect their immigrant neighbors from the Trump administration's campaign of mass deportations should decline to participate in Flock's or any other LPR company's nationwide data sharing operation.

What Success Looks Like

Protecting both your residents' civil rights and civil liberties and the fundamental purposes of Massachusetts law requires only two straightforward actions:

1. **Disable automated data sharing** with entities outside Massachusetts through Flock's or other LPR provider administrative settings.

---

[5] Nancy Guan, Local law officers must cooperate with ICE. What that may mean for the public, WUSF Public Media (Feb. 12, 2025), https://www.wusf.org/politics-issues/2025-02-12/local-officers-must-cooperate-ice-what-that-means-for-public.

[6] Gisela Salomon and Kate Payne, Detained immigrants at 'Alligator Alcatraz' say there are worms in food and wastewater on the floor, Associated Press (Jul. 11, 2025), https://apnews.com/article/alligator-alcatraz-immigration-detainees-florida-cc2fb9e34e760a50e97f13fe59cbf075.

[7] Nermeen Shaikh, Shirsho Dasgupta, and Thomas Kennedy, Where Are the Detainees? Hundreds of 'Alligator Alcatraz' Prisoners Disappear from ICE Database, Democracy Now (Sept. 25, 2025), https://www.democracynow.org/2025/9/25/alligator_alcatraz.

2. **Amend contract language** that may give Flock or another LPR company the legal right to share your residents' data with law enforcement outside the Commonwealth.[8]

These are the only ways to ensure information collected by your police department's technology will not be misused by another agency or used in contravention of the protections of the Shield Law. Ending nationwide data sharing also reduces the likelihood that information collected by your police department will be used for civil immigration enforcement or other unintended purposes.[9]

If your police department claims they are not sharing data nationwide, we recommend requesting documentation showing their current LPR database settings and complete contract terms to verify compliance with the above principles.[10]

If external sharing of license plate reader data cannot be prevented through both restrictive system settings and clear contract language limiting external data sharing, your municipality should end its contract with Flock Safety or other LPR providers.

ACLU Support Available

ACLU of Massachusetts staff are available to meet with you and your police chief to review your current Flock or other LPR settings and contract language. We can provide technical assistance to protect civil rights and civil liberties while addressing public safety concerns. Please email gepstein@aclum.org if you have questions about license plate readers in your community.

We request a response within 30 days regarding the steps your municipality is taking to address this issue.

Thank you for your public service and your dedication to the people of Massachusetts.

Sincerely,

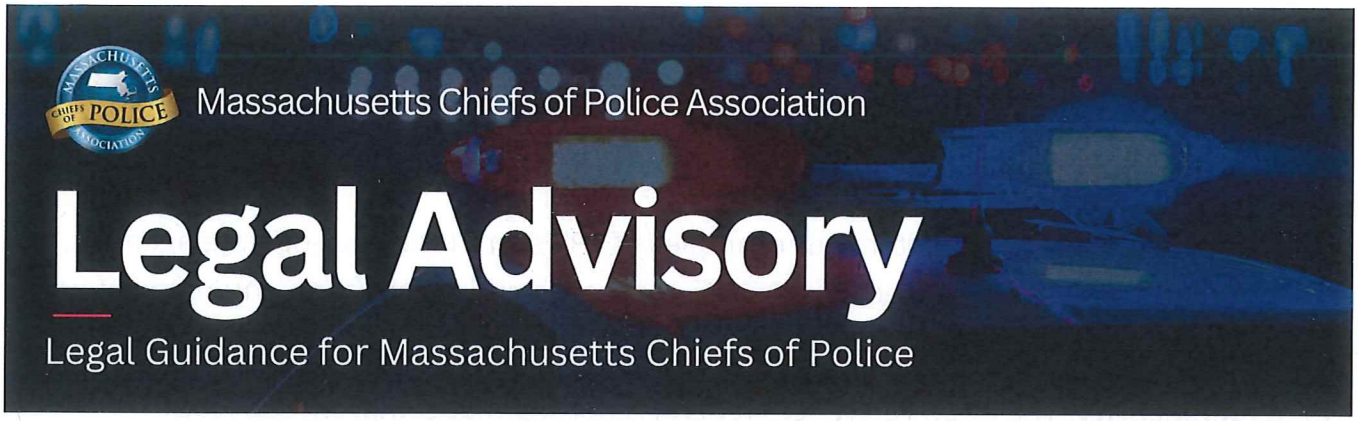
Kade Crockford, Director, Technology and Justice Programs, ACLU of Massachusetts
Gideon Epstein, Policy Counsel, Technology for Liberty Program, ACLU of Massachusetts

---

[8] For more information about contract language, please visit: https://data.aclum.org/2025/10/07/flock-gives-law-enforcement-all-over-the-country-access-to-your-location/

[9] The same concerns apply to police department use of other LPR technology, including systems provided by Vigilant Solutions, a Motorola subsidiary.

[10] Note that disabling nationwide automatic sharing does not prevent cooperation on specific investigations. Your department can still choose to share data with named departments or agencies when appropriate. The key difference is that this sharing would be deliberate and reviewable rather than automatic and unmonitored.



ACLU Letter Regarding License Plate Readers (LPRs)

Many Massachusetts law enforcement agencies have received a letter from the ACLU of Massachusetts concerning the use of Flock Safety and other vendor-hosted license plate reader (LPR) systems. This advisory provides an overview of the issues raised by the ACLU, identifies key legal considerations for Massachusetts agencies, and outlines steps agencies may consider in coordination with municipal or campus counsel.

This advisory is educational. It does not direct agencies to take or refrain from any specific action. Each agency should consult with counsel regarding its contracts, system configurations, policies, and operational practices.

Brief Summary of the ACLU Letter

The ACLU letter raises several concerns regarding agency use of Flock Safety and other vendor-hosted LPR systems. In summary, the ACLU asserts the following:

- ☐ **Nationwide Data Sharing:** Flock's system may allow agencies to share Massachusetts-generated LPR data with thousands of law enforcement agencies nationwide and to search data those agencies contribute.
- ☐ **Contract Language:** Some publicly available Flock template agreements in other jurisdictions contain broad, long-term license terms that allow the vendor to use or disclose "Agency Data" in ways the ACLU believes may exceed what an agency intends based on its user-selected sharing settings.

- ☐ **Massachusetts Shield Law:** The ACLU argues that automatic nationwide sharing could conflict with G. L. c. 147, section 63 if out-of-state agencies access Massachusetts LPR data in connection with investigations involving reproductive or gender affirming health care that is lawful in Massachusetts.
- ☐ **Out-of-State Uses:** The letter cites examples of LPR searches by out-of-state agencies, including searches conducted by agencies engaged in civil immigration enforcement and searches related to abortion activity in another state.
- ☐ **Cybersecurity:** The ACLU references federal reporting that compromised Flock credentials have been found on criminal forums, raising concerns about unauthorized access.
- ☐ **Requested Municipal Actions:** The ACLU asks municipalities to disable nationwide sharing, amend contracts to restrict vendor disclosure, consider ending contracts if amendments are not possible, and respond within thirty days.

Key Legal & Operational Considerations

The following considerations are intended to help agencies frame internal discussions with counsel. This section is not an exhaustive legal analysis.

Constitutional Considerations

Massachusetts courts have recognized that prolonged or comprehensive location tracking may implicate privacy rights under Article 14 and federal law. LPR technology is lawful when used for legitimate law enforcement purposes and when coupled with appropriate oversight, documentation, and other retention controls. Agencies should ensure that their use of LPR data does not result in long-term tracking without a valid legal basis.

Massachusetts Shield Law

The Shield Law in G.L. c. 147, section 63 limits the ability of Massachusetts agencies to provide information or assistance to out-of-state or federal investigations involving reproductive or gender affirming health care that is lawful in Massachusetts, subject to specific exceptions. There is currently no Massachusetts case interpreting how this statute applies to vendor-hosted, nationwide LPR platforms. Automated sharing that allows out-

of-state agencies to run queries against Massachusetts LPR data may raise Shield Law questions depending on how a court interprets 'information' or 'assistance' in this context.

Civil Rights & Immigration Considerations

The ACLU letter describes examples of LPR searches conducted by out-of-state agencies involved in civil immigration enforcement. Automatic nationwide sharing may result in Massachusetts data being used by agencies operating under legal frameworks and policy environments that differ from those in Massachusetts. Agencies should be aware of these potential implications when evaluating data sharing settings.

Contractual Rights & Vendor Practices

Publicly available Flock contracts in other jurisdictions vary in how they address data ownership, vendor license rights, and disclosure authority. Some Massachusetts agencies appear to have negotiated more restrictive terms. Agencies should rely on their actual contracts and should not assume that template language applies. Counsel should review:

- ☐ ownership and control of LPR data
- ☐ vendor license and use rights
- ☐ vendor disclosure authority
- ☐ compliance obligations regarding Massachusetts law, including the Shield Law
- ☐ retention, deletion, auditing, and breach notification provisions

Cybersecurity & Account Management

Externally hosted systems require strong access controls. Federal reporting of compromised LPR credentials highlights the importance of multi-factor authentication, careful user account management, regular audits, and appropriate administrative restrictions.

Suggested Steps for Agencies

The following steps are advisory and should be taken in coordination with agency counsel.

- ☐ **Notify Counsel and Leadership:** Agencies should promptly notify their municipal or campus counsel, city or town administrator, and appropriate IT or procurement officials.

Counsel should review the ACLU letter, this advisory, and any contracts or system configurations related to LPR use.

- ☐ **Inventory Current LPR Usage:** Agencies should identify:
  - the LPR vendor or vendors used
  - current data sharing settings
  - retention settings
  - audit logs, if available, that show which outside agencies have accessed Massachusetts data
  - any internal directives, policies, or memoranda governing system use
- ☐ **Review Contracts with Counsel:** Counsel should review:
  - ownership of collected data
  - vendor rights to use or disclose data, and for what purposes
  - contractual requirements regarding adherence to agency-selected sharing settings
  - obligations to comply with Massachusetts law, including the Shield Law
  - audit, retention, deletion, and breach notification requirements.

  Counsel may, as appropriate, recommend amendments that clarify ownership, restrict disclosure, or limit vendor sharing of Massachusetts data with out-of-state agencies unless consistent with applicable law and lawful process.
- ☐ **Review Sharing Configurations:** Agencies should confirm their existing sharing settings and determine, with counsel, whether continued nationwide or out-of-state sharing aligns with statutory requirements, policy considerations, and operational needs. Some municipalities may determine that limiting sharing to in-state or specifically identified partners better aligns with local risk assessments.
- ☐ **Update Internal Policies:** Agencies should ensure that internal LPR policies address:
  - authorized uses
  - documentation requirements for searches
  - retention limits

- access controls and procedures
- supervisory review and audit requirements
- restrictions on sharing or assistance inconsistent with the Shield Law

☐ **Coordinate Any Response to the ACLU:** Any written response to the ACLU should come from the municipality's authorized legal or administrative official. Responses may acknowledge receipt of the letter, confirm that the municipality is reviewing the issues with counsel and relevant officials, and avoid making legal commitments that have not been reviewed and approved by counsel.

Conclusion

The ACLU letter raises important questions about nationwide sharing of LPR data, vendor practices, contract terms, Shield Law compliance, civil rights implications, and cybersecurity. LPR technology remains a lawful and effective investigative tool in Massachusetts when used with appropriate safeguards. The key issues for agencies are their contract terms, current data sharing and retention settings, and whether vendor-hosted systems operate in ways that align with Massachusetts law and local policy objectives.

MCOPA encourages all agencies to work with counsel to review these matters carefully and to ensure that local practices, policies, and agreements reflect current legal requirements and operational needs.

This advisory is informational and does not constitute legal advice. Agencies should consult their legal counsel regarding their specific circumstances.

Massachusetts Chiefs of Police Association, Inc.
Office of the General Counsel
legal@masschiefs.org
(774) 293-2658
353 Providence Road | South Grafton, MA 01560

(Rev. 11.17.2025)