Massachusetts Data Breach Settlement: A Wake-Up Call for Rental Housing Operators

August 28th, 2025 | and Jay Harris

On August 19, 2025, the Massachusetts Attorney General announced a $795,000 settlement with Peabody Properties, Inc., a Braintree, Massachusetts-based property management company, over serious failures in its handling of cybersecurity breaches and breach notifications. Between November 2019 and September 2021, Peabody experienced five separate phishing-based cyber intrusions that exposed sensitive personal information—including Social Security numbers, driver's license data, and bank account details—of nearly 14,000 Massachusetts residents. The Attorney General found that Peabody unlawfully delayed notifying both the Attorney General's Office and affected individuals, with the first two incidents not disclosed until nearly seven months after discovery.

The proposed consent judgment, awaiting court approval, requires Peabody to pay $795,000 in penalties and to implement a comprehensive suite of security measures: multi-factor authentication, phishing protection tools, vulnerability management, asset inventory, intrusion detection and prevention, and ongoing annual security assessments for three years. The case underscores not only the financial and reputational costs of poor breach response, but also the regulatory expectation that Massachusetts property managers, like a wide range of other covered businesses, safeguard renter and applicant information.

For Massachusetts property operators, this settlement is a reminder of the strict requirements of the state's Security Breach Notification Law (G.L. c. 93H) and Data Security Regulations (201 CMR 17.00). These laws require prompt notice to the Attorney General, the Office of Consumer Affairs and Business Regulation (OCABR), and affected residents whenever a breach of security occurs involving personal information. Notice cannot be unreasonably delayed, even if the full scope of affected individuals is not yet known. Massachusetts law also mandates that companies offering housing or financial services, among other businesses, maintain a Written Information Security Program ("WISP") with administrative, technical, and physical safeguards appropriate to the size and nature of the business.

Well-run operators should take proactive steps to avoid Peabody's mistakes. First, boards and executives must treat cybersecurity as a core compliance function, not a back-office IT issue. That means adopting and regularly updating a WISP, running phishing simulations and staff training, and implementing layered defenses such as endpoint protection, encryption, and multi-factor authentication. Second, incident response plans should be in place and tested—so that the organization can identify, contain, and report breaches quickly. Under Massachusetts law, "as soon as practicable and without unreasonable delay" means days, not months.

Equally important, organizations should create executive-level reporting structures for data security. Senior leadership should receive periodic briefings on vulnerability assessments, system monitoring, and regulatory obligations, to prevent regulatory gaps and ensure consistent protections across business lines.

The Peabody case should be viewed as a cautionary tale. In an environment where renters, applicants, and customers entrust companies with their most sensitive identifiers, Massachusetts regulators will not tolerate delay or inadequate protections. Executives of property management companies should consider this settlement an opportunity to re-evaluate their data security posture, confirm that breach response protocols align with Massachusetts law, and allocate resources to meet both the letter and the spirit of state data security regulations.