AN A.S. PRATT PUBLICATION
MAY 2025
VOL. 11 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 4** **May 2025**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

E-Verify in Illinois: SB0508 Myths Dispelled, Rights Protected

By Dawn M. Lurie*

In this article, the author discusses the Illinois "Right to Privacy in the Workplace Act."

The passage of the vaguely named "Right to Privacy in the Workplace Act" led to widespread chatter that the law possibly prohibited employers from using E-Verify unless they were explicitly required to do so under federal law. The Illinois Department of Labor (IDOL) recently clarified what the law requires.

BACKGROUND

Illinois first implemented the E-Verify provisions in the Right to Privacy in the Workplace Act[1] under Public Act 95-138 in 2008, with an amendment in 2010. Now, new amendments under Public Act 103-879, effective January 1, 2025, further update the law.[2]

Key changes include mandatory employee notification related to Form I-9 inspections (remarkably similar to obligations in the state of California), protection against retaliation for exercising rights under E-Verify, and specific corrective action opportunities for employees with tentative nonconfirmations. Employers must also adhere to strengthened anti-discrimination provisions, ensuring that E-Verify is used fairly and transparently.

On October 29, IDOL issued a much welcomed FAQ on the Right to Privacy in the Workplace Act (SB0508 or the Act). It addresses the widespread misinformation and misunderstanding about SB0508's impact on E-Verify in Illinois and was created by IDOL in response to policy clarification requests.

Most notably, the new FAQ clarifies that SB0508 does not prohibit employers from voluntarily use of E-Verify for employment verification.

The IDOL FAQs[3] help Illinois employers better understand their obligations under SB0508. FAQ #4 reads:

Q. May Illinois employers choose to voluntarily use E-Verify?

---

* The author, senior counsel based in the Washington, D.C., office of Seyfarth Shaw LLP, may be contacted at dlurie@seyfarth.com.

[1] https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2398&ChapAct=820%A0ILCS%A055/&ChapterID=68 &ChapterName=EMPLOYMENT&ActName=Right+to+Privacy+in+the+Workplace+Act.

[2] https://ilga.gov/legislation/publicacts/fulltext.asp?Name=103-0879.

[3] https://labor.illinois.gov/faqs/right-to-privacy-in-the-workplace-e-verify.html.

> A. Yes. Illinois law does not prohibit any employer from using E-Verify. However, employers who use E-Verify must follow the requirements of the Right to Privacy in the Workplace Act.

The FAQ goes on to remind employers that "as of January 1, 2025, prior to enrolling in the E-Verify System, employers are urged to consult the Illinois Department of Labor's website for current information regarding the accuracy of the program."

The FAQ also encourages employers to review and understand their legal responsibilities regarding E-Verify. Employers are also reminded that the Act prohibits misuse of E-Verify and imposes specific training and recordkeeping requirements on employers. The FAQ also discusses E-Verify participation posting requirements, an employer's obligation in the event of a discrepancy in an employee's employment verification information, and how to file a complaint.

WHAT IS THE COST OF NON-COMPLIANCE?

State investigations remain complaint-driven, with significant increases in monetary fines for willful and knowing violations of the Act, along with broadly defined penalties. Courts may award actual damages plus costs to the charging party and can impose additional penalties. These penalties are nebulously outlined: "In determining the amount of the penalty, the appropriateness of the penalty to the size of the business of the employer charged and the gravity of the violation shall be considered. The penalty may be recovered in a civil action brought by the Director in any circuit court." It remains unclear how SB0508 will be enforced.

WHAT ARE KEY PROVISIONS IN SB0508 AND THE 2025 AMENDMENTS?

Voluntary Use of E-Verify

The FAQ reaffirms that Illinois employers may voluntarily use E-Verify, provided that the employer follows the requirements outlined in the Act. As mentioned above, there is no ban or restriction against the voluntary use of E-Verify in Illinois, countering any contrary assumptions or misinformation.

Enhanced Worker Protections

SB0508 expands worker protections by requiring employers to:

- *Follow Updated Notification Timelines*. When an employer receives notification from a federal or state agency of a discrepancy as it relates to work authorization, including a tentative nonconfirmation (TNC) from E-Verify, the law reiterates the E-Verify rule that no adverse action should be taken.

  Additionally, it adds a requirement that employers provide written notice of the issue to the employee pursuant to the following guidelines:

- Notice should be given via hand-delivery if possible, or alternatively by mail and email within five business days, unless federal law or a collective bargaining agreement specifies a shorter timeline.
- Note that currently, E-Verify provides a 10-day period to deliver the notice and take action but does not mandate specific timing for the notification.
- The notice must include an explanation of the determination, the time period for the employee to notify the employer if they wish to contest the determination, the time and date of any meeting with the employer or with the inspecting entity, and notice that the employee has the right to representation.
- If requested by the employee, the employer must provide the original notice from the federal or state agency within seven business days (note: E-Verify rules already require employers to deliver the "Further Action Notice" to employees).

- *Notify Employees of Form I-9 and Employment Record Inspections*. Employers must inform employees if their Form I-9 documentation will be inspected. Specifically, employees must be notified of any inspection within 72 hours of receipt, and where appropriate, employee representatives should also be notified. Per the law's requirement, IDOL will develop and publish a template posting notice that employers may use to comply with this requirement.

- *Notify Employees of Discrepancies or Suspect Document Determinations Made By Inspecting Entities, Generally Homeland Security Investigations (HSI)*. Once the inspection is completed, employees should have an opportunity to resolve any verification discrepancies. Employers must notify the employee within 5 business days (or sooner if federal law or a collective bargaining agreement requires). The notification must be hand-delivered. If hand delivery is not possible then SB0508 requires that the notice be sent by mail and email (provided the email address of the employee is known). The notice must include information such as:
  - An explanation of the potential invalidity of the employee's work authorization documents;
  - A timeframe to respond if they wish to contest;
  - Details of any scheduled meetings regarding the issue, if known; and
  - Information about their right to representation at these meetings. There are also timelines for providing information to employees if the determination was contested which include onerous requirements such as providing a redacted original notice from the inspecting

entity within 7 business days (when such notice is requested by the employee).

It is likely that the hand delivery and snail mail mandates, specifically with respect to E-Verify TNCs, will prove extremely burdensome for employers, especially those that utilize electronic onboarding and I-9 systems. Further clarification from IDOL would be welcomed.

Unlike SB0508, HSI does not dictate the timeline to notify employees, but rather expects employers to fully address a Notice of Suspect Documents (NSD) within 10 days – either by terminating the employee or ensuring alternative documents are actively under HSI review within this period for those that "contest" the findings.

Specifically, when HSI issues an NSD, both the employer and the affected employee(s) are given an opportunity to provide evidence of valid U.S. work authorization if they believe HSI's findings are incorrect. The 10 day timeline, which incidentally is not required by regulation, is tight: employees must respond promptly by presenting alternative documentation, which the employer then submits to HSI for further review. In some cases, HSI agents may request direct meetings with employees to verify their status.

Existing Procedural Requirements

The existing Illinois law mandates that employers and authorized agents using E-Verify adhere to a structured process involving:

- *Employer Certifications*: Employers must certify compliance with Illinois-specific E-Verify guidelines upon enrolling in the program. This certification affirms understanding of state-specific rules, including employee notification requirements and anti-discrimination provisions. Specifically, employers must affirm that they have received the E-Verify training materials from the Department of Homeland Security (DHS) and that they have posted the required E-Verify participation and anti-discrimination notices in a prominent place that is clearly visible to prospective employees.
- *Training, Testing, and Certification:* Further, all employees who will administer the program must complete the E-Verify Computer-Based Tutorial or equivalent with the appropriate training modules. Users must be certified as having successfully completed training and testing before accessing and using E-Verify. E-Verify offers this training and mandates completion for all new users prior to being allowed into the system. Web services providers are obligated to create (based on USCIS guidance) these materials and related trainings and associated knowledge tests.

Employers must maintain proof of meeting these notification, testing, training, and documentation obligations. Although these requirements already exist in Illinois law,

they have often been overlooked by employers. The recent amendments emphasize the importance of following these guidelines to ensure fair treatment of employees and at the same time remain compliant with E-Verify obligations.

IDOL published the required Employer Attestation Form,[4] which employers must use to certify compliance with certification requirements. Employers should complete this attestation upon initial enrollment in E-Verify or, for existing participants, they should have completed this attestation by January 31, 2025. Submission to IDOL is not required. If an employer misses the deadline, the employer should complete the attestation as soon as possible to ensure compliance.

WHAT DO EMPLOYERS IN ILLINOIS NEED TO KNOW?

Maintaining Compliance

Employers using E-Verify in Illinois should familiarize themselves with these updates to ensure compliance and safeguard worker rights. Notably, E-Verify remains permitted in Illinois, so employers can continue using it without concern. While minor adjustments to compliance processes may be necessary for some, many of the law's new safeguards are already required by federal E-Verify rules.

Audits and Investigations

In cases where an employer is audited by Homeland Security Investigations or is under investigation by the Department of Labor (DOL) or the Department of Justice's Immigrant and Employee Rights (IER) section, additional notification requirements and timelines will apply. Employers facing such scrutiny should consult competent legal counsel to navigate these situations and ensure full compliance.

RECOMMENDED ACTIONS FOR ALL E-VERIFY EMPLOYERS

With these changes in mind, Illinois employers should take this opportunity to review and, if necessary, update their E-Verify processes and procedures. In fact, all employers could benefit from an E-Verify review. Steps to consider include:

- *Reviewing E-Verify Account Structures*. Ensuring E-Verify accounts are set up correctly in terms of entities and locations while also ensuring accounts are accessible only to those who have completed the mandatory training.
- *Maintaining "E-Verify Hygiene."* Ensuring that cases have been timely closed, that all new hires at participating hiring sites have been processed through the system, including those initially delayed by receipts or temporary documents, and that mismatches are timely addressed.

[4] The Attestation can be found at: https://labor.illinois.gov/content/dam/soi/en/web/idol/laws-rules/legal/documents/EVerify%20Attestation%20Form.pdf.

- *Updating the MOU with E-Verify*. Ensuring the registered locations, the required Points of Contact, and the number of employees are accurate, along with the employer's Federal Contractor status, if applicable.

- *Review for Trends and Red Flags*. Employers should run E-Verify reports and pay attention to the Dashboard. For example: do you have a user that is opening and closing multiple cases for the same employee? Do you have open TNCs? Do you have employees with Final Nonconfirmations still working for you?

USCIS's Account Compliance branch is conducting an increasing number of Desk Review audits on accounts, which heightens the need for accurate, up-to-date account management practices. By maintaining accurate and readily accessible records and following E-Verify protocols, employers can help avoid compliance issues and continue to benefit from the program. While E-Verify may not be suitable for every employer, it stands as a best practice for supporting a legally compliant workforce.

LOOKING AHEAD

SB0508 strives to ensure transparent, fair, and lawful employment verification practices, but at the same time this law creates a number of onerous requirements for employers.