



**AMERICAN SOCIETY OF
CRIME LABORATORY DIRECTORS, INC.®**

65 Glen Road, Suite 123, Garner, NC 27529

August 6, 2026

ASCLD BOARD OF DIRECTORS

Claudine Carter Pereira, President
Broward Sheriff's Office
Crime Laboratory

Kerri T. Heward, President-Elect
San Bernardino County Sheriff's
Department – Scientific Investigations
Division

Julie Conover Sikorsky, Secretary
Palm Beach County Sheriff's Office
Crime Laboratory

Brian Hoey, Treasurer

Scott Hummel, Past President
Kansas City Police Department

Lori Nix
Georgia Bureau of Investigation -
Division of Forensic Sciences

Laura A. Tramontin
NJSP Office of Forensic Sciences

F. Wayne Lewallen
North Carolina State Crime Laboratory

Mandy Tinkey
Allegheny County Office of the Medical
Examiner & Division of Forensic
Laboratories

Jason R. Bundy
Florida Department of Law
Enforcement

Robin J. Woolery
Illinois State Police

Meredith Rosenberg
NYC OCME, Department of Forensic
Biology

Grant M. Belancik
Arizona Department of Public Safety

ASCLD STAFF

John A. Byrd, BG (Retired)
Executive Director

Ramona Robertson
Administrative Assistant

**ASCLD Notification Regarding Electronic DNA Data File
Security**

The American Society of Crime Laboratory Directors (ASCLD) is sharing information regarding a recently identified security concern involving certain electronic data files generated and used in forensic DNA analysis.

Modern forensic DNA workflows rely on electronic files generated through capillary electrophoresis and subsequently evaluated using DNA analysis software. Recent independent testing demonstrated that, under specific circumstances, information contained within certain files generated by select Applied Biosystems™ Human Identification data-collection software and analyzed using GeneMapper™ ID-X Software could potentially be modified without producing an immediately apparent indication that the file had changed.^[1-3] Examples of the affected file types include .fsa and .hid files.^[2, 3]

The demonstration identifies a potential vulnerability in the security protections historically associated with these electronic files.^[2, 3] Exploitation would require access to the files or the systems on which they are maintained, together with sufficient knowledge and intent to alter the data.^[1, 3]

Thermo Fisher Scientific has stated that it is not aware of unauthorized file modification in a customer environment.^[1] The identification of a potential method by which a file could be modified does not establish that any laboratory data have been compromised, nor does it inherently call into question the validity or reliability of previously reported forensic DNA results. The identified concern relates to the electronic data files; it does not alter the underlying physical evidence or biological sample.^[1]

Thermo Fisher Scientific has released security updates for certain affected versions of Applied Biosystems Data Collection and instrument software, as well as GeneMapper ID-X Software.^[2,3] The updates incorporate digital signatures intended to help customers verify that files have not been modified between their generation and subsequent analysis.^[3]

ASCLD Notification Regarding Electronic DNA Data File Security
August 6, 2026

ASCLD encourages Thermo Fisher Scientific to make security patches or functionally equivalent updates available at no additional cost, for legacy versions of the GeneMapper ID-X and affected Data Collection software.

ASCLD is providing this notification so that laboratory leaders are aware of the concern and the availability of additional security features. Each laboratory should consider this information in the context of a risk assessment of its own instrumentation, software, information-technology environment, access controls, and existing quality practices and determine whether further review or action is appropriate.

ASCLD will continue to follow developments and share relevant information with the forensic science community as it becomes available.

References

Online references accessed August 5, 2026.

1. Mariah Timms, "Security Flaw Placed 30 Years of DNA Evidence at Risk of Hacking," The Wall Street Journal, August 2, 2026.

2. Cybersecurity and Infrastructure Security Agency. "Thermo Fisher Applied Biosystems Genetic Analyzers." ICS Medical Advisory ICSMA-26-216-01, August 4, 2026.

3. Thermo Fisher Scientific, "Genetic Analyzer Instrument Data Collection and GeneMapper ID-X Software (select versions)," Security Bulletin, July 31, 2026.