Security Incident Handling Procedure Guide

July 2017
Version 9.6

DRAFT

Based on NIST Special Publication 800-61, Computer Security Incident Handling Guide, this manual establishes procedures for handling Security Incidents that may compromise the availability, integrity and confidentiality of Equifax data and resources.

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000574

Document Change Management

Document Name	Security Incident Handling Procedure Guide		
Type:	Policy & Procedures	**Equifax Policy No.**	
Policy Owner:	Berlene Herren	**Issued By:**	Global Security
Approved By:	Stephen Cosby, Susan Mauldin	**Prepared By:**	Amanda Le
Effective Date:	June 2007		
Last Reviewed Date:	July 2017	**Next Review Date:**	July 2018

VERSION CONTROL

Date	Name	Version	Description of Changes
May 2006	Nick Nedostup	1	Production document created.
June 2008	N. Nedostup, D. Amster, S. Choffery	6	Updated to combine Technical, Data and Physical Security Plans into one unified Security Incident Response Plan.
February 2009	N. Nedostup, D. Amster, S. Choffery	7	Yearly Updates
February 2010	N. Nedostup, D. Amster, S. Choffery	8	Yearly Updates
February 2011	N. Nedostup, D. Amster, S. Choffery	9	Yearly Updates
October 2011	N. Nedostup, D. Amster, S. Choffery	9.1	Updated to reflect organizational/employee changes. Added Document Change Management Section.
November 2011	N. Nedostup	9.1	Updated Section 3.1 to include frequency of IR Contact List review & updates.
March 2012	Ray Strubinger	9.1.2	Updated Appendix F and created a separate document for the information. Verified web addresses. Minor corrections to wording and terminology.
October 2012	Ray Strubinger	9.3	Update to DDoS procedure
June 2014	Francis Finley	9.4	Update to correct grammar, formatting, clarify language, and organization restructuring.
October 2014	Francis Finley	9.5	Update to fix section on Forensics/Malware handling, include additional contacts, Archer ticketing information.
October 2014	Ted Mac Daibhidh, CD	9.5.1	Standardized formatting throughout document; corrected various errors; restructured lists to be easier to reference/read, resized figures to be more readable; changed heading font and colors to match official template document; corrected "single point lists"; updated ToC.
October 2015	Susan Mauldin	9.5.1	Reviewed with no revisions
October 2016	Susan Mauldin	9.5.1	Reviewed with no revisions
July 2017	Morphick, Francis Finley, Berlene Herren, Amanda Le, Michael Douglas, Stephen Cosby, Bryce Williams	9.6	General cleanup, Added CAT Triage, IR best practices, and Kill Chain model, document name change from "Security Incident Handling Policy & Procedure Guide" to "Security Incident Handling Procedure Guide"

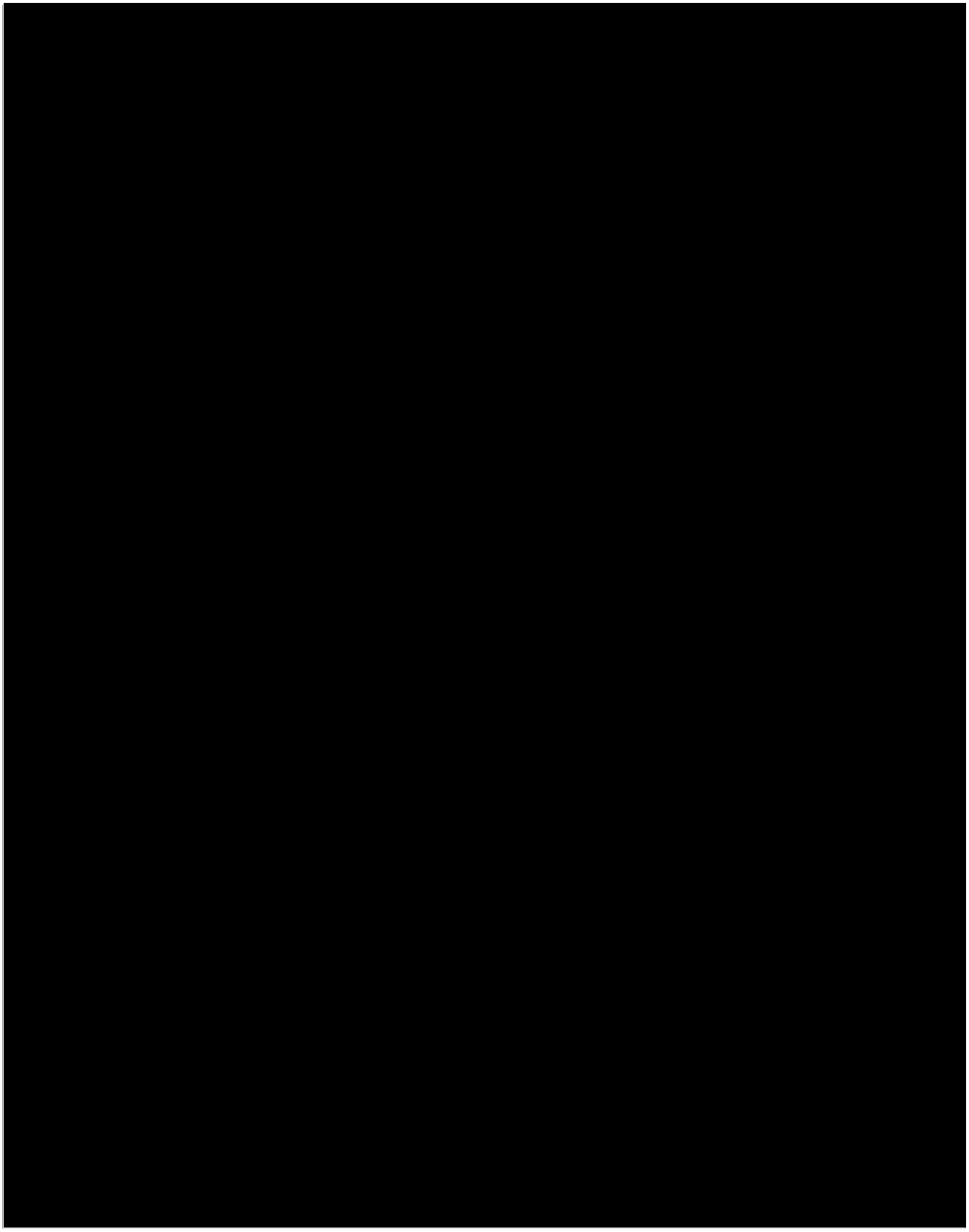
DRAFT

CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000575

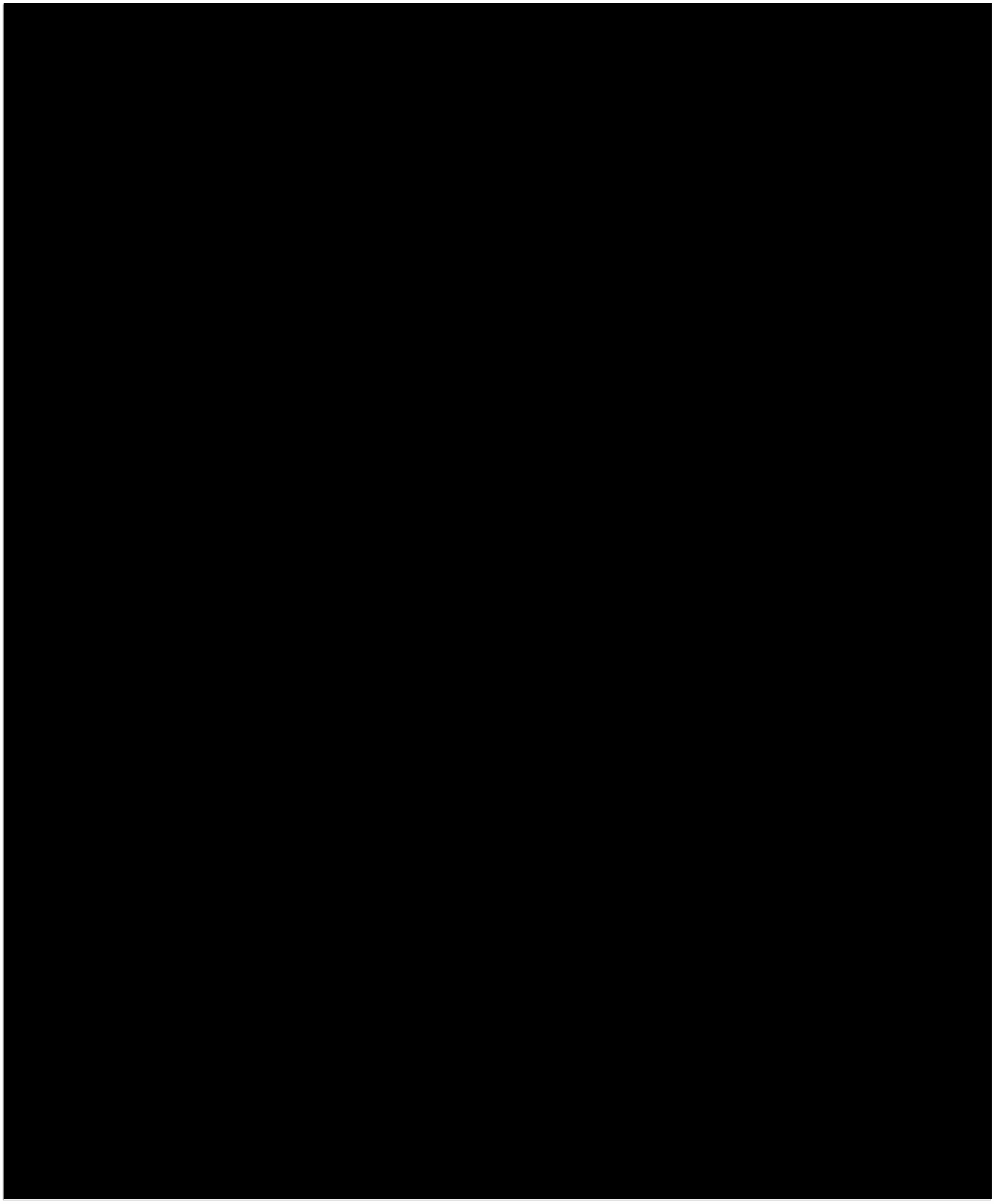
Table of Contents

DRAFT

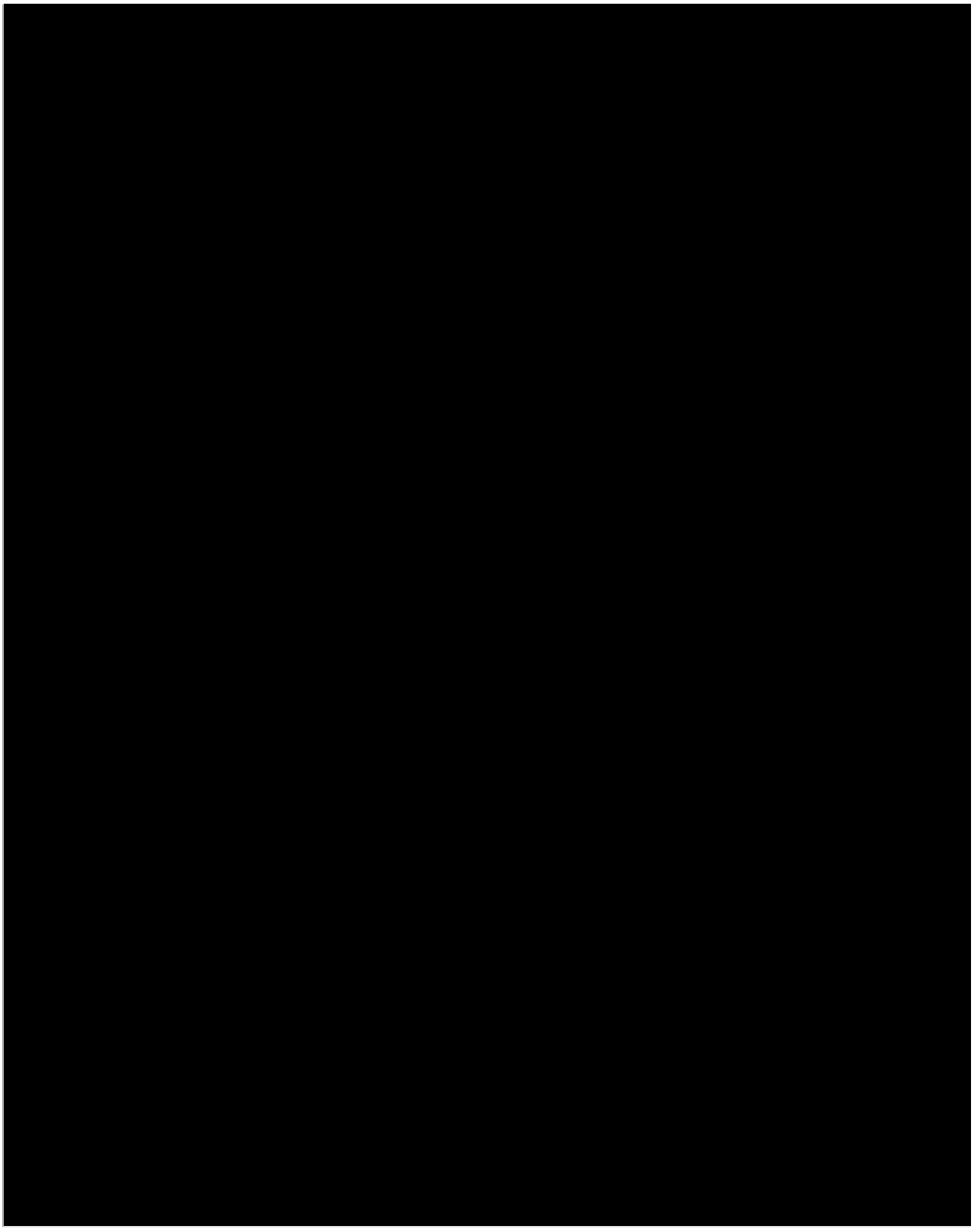
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000576



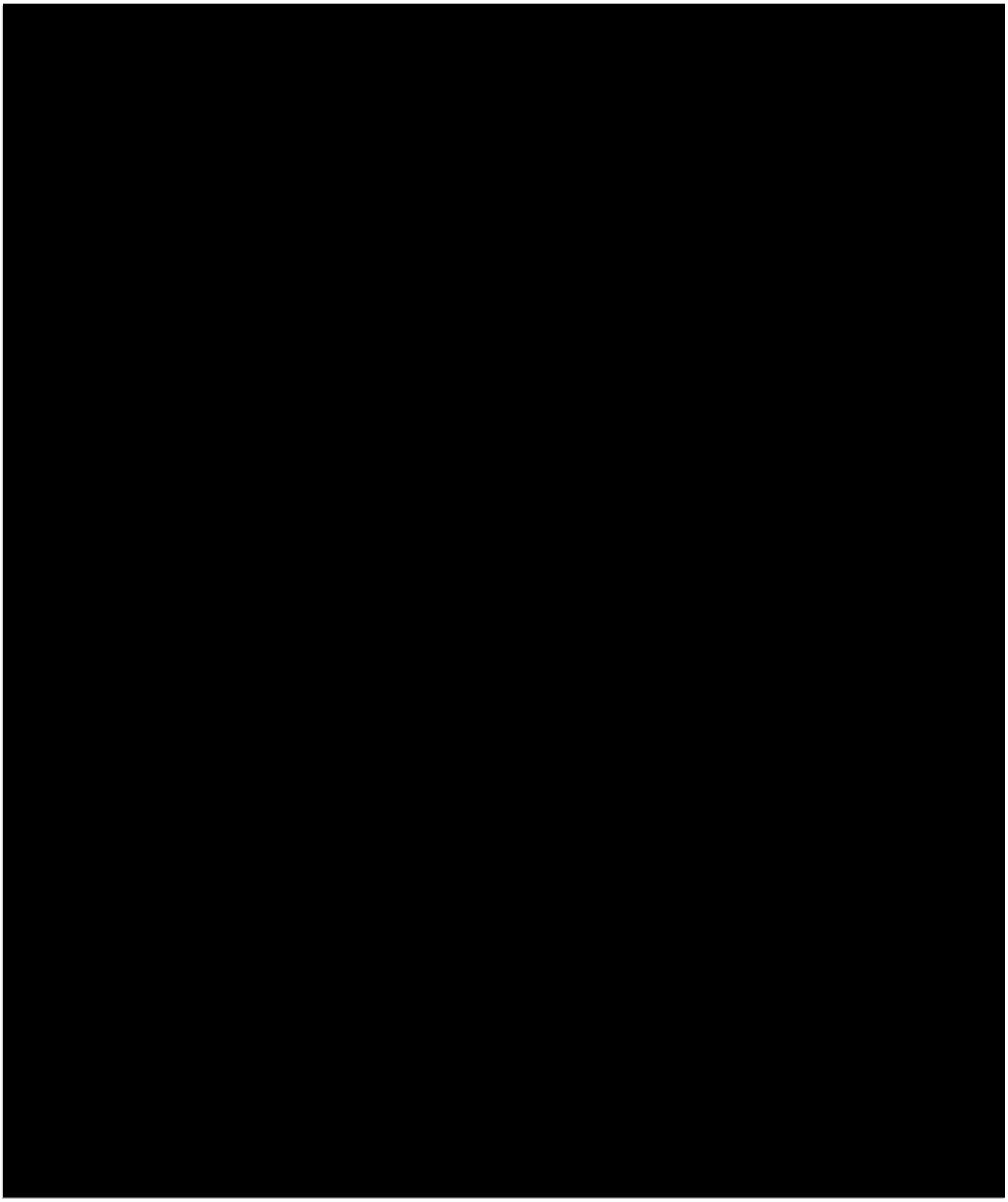
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000577



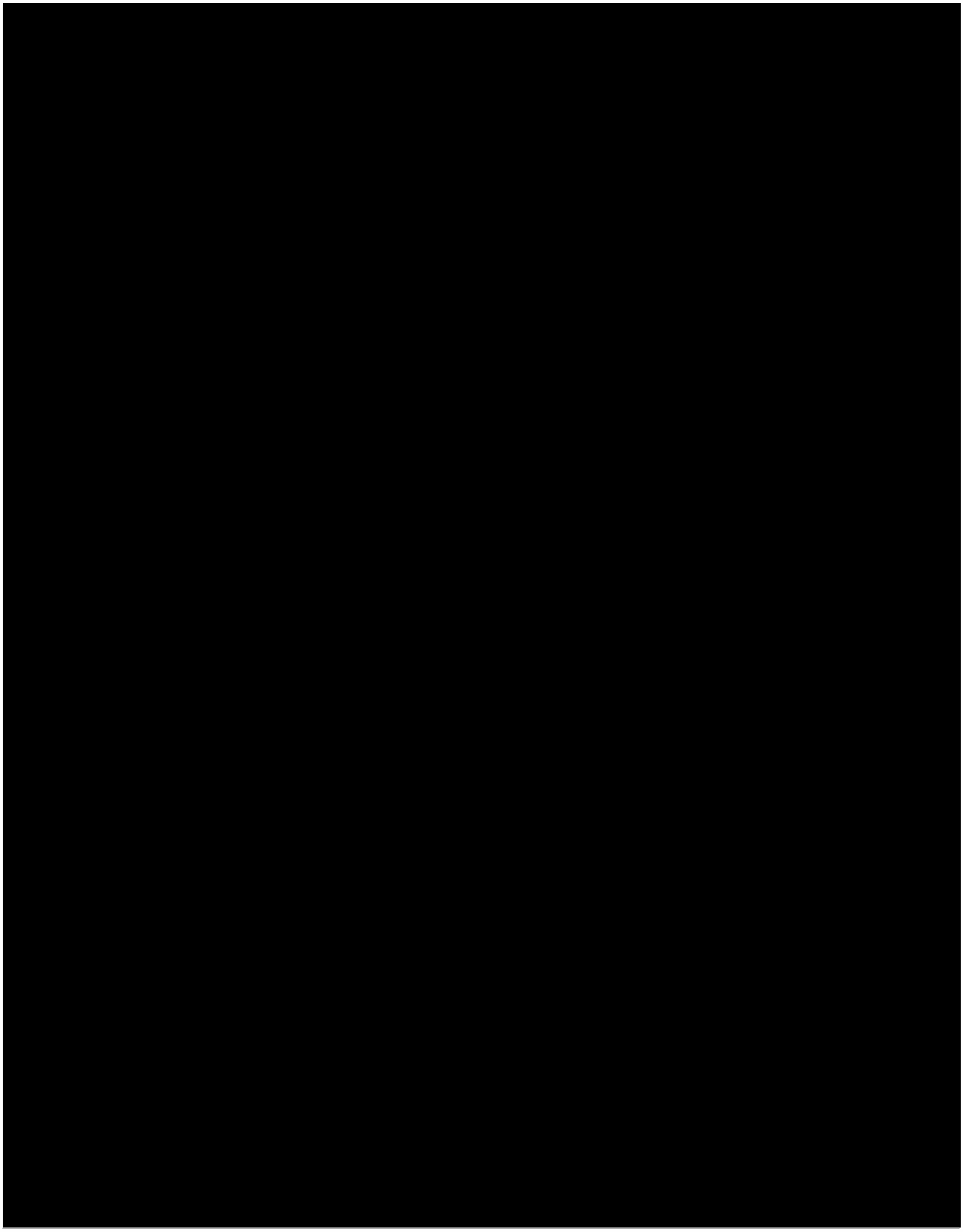
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000578



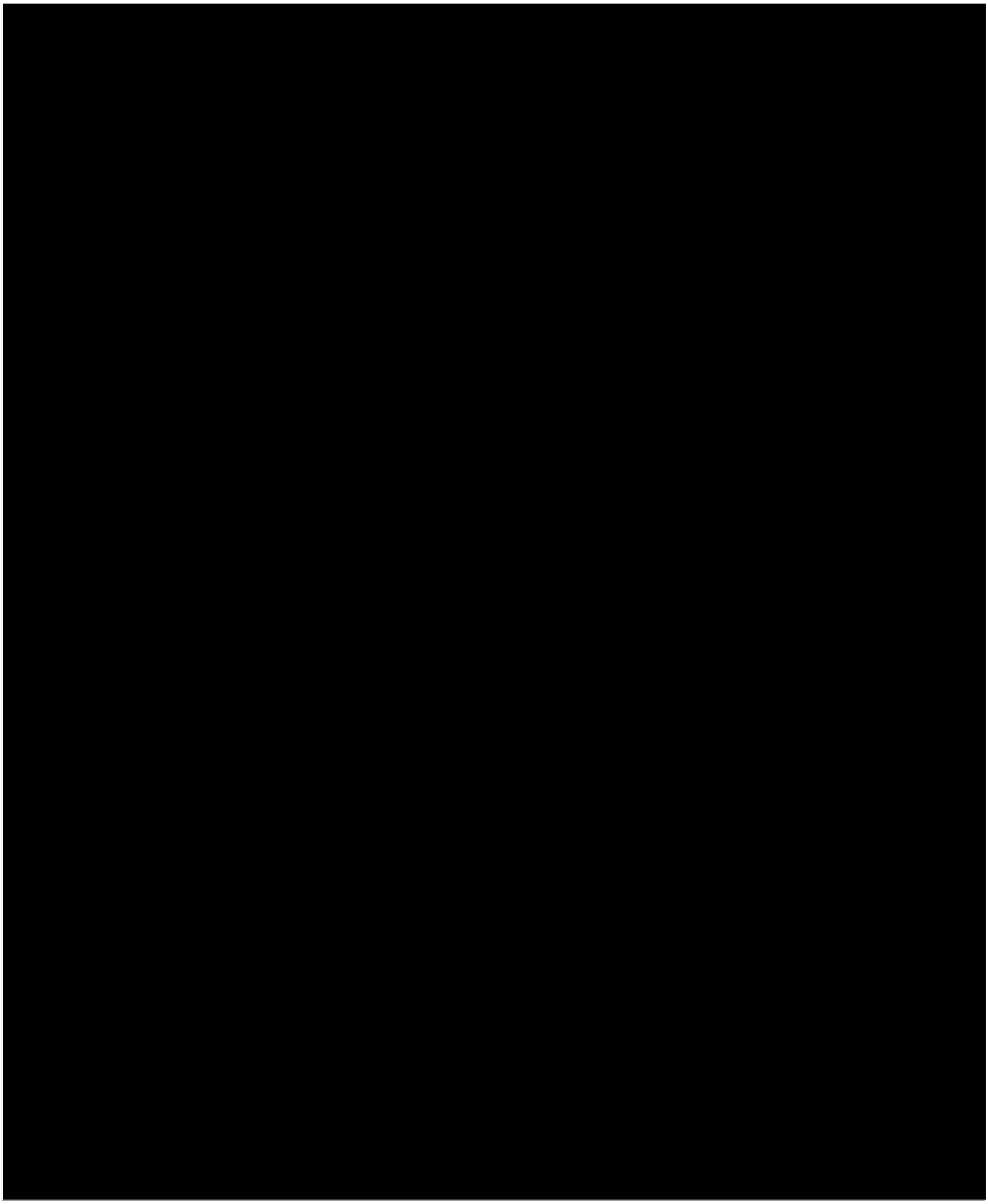
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000579



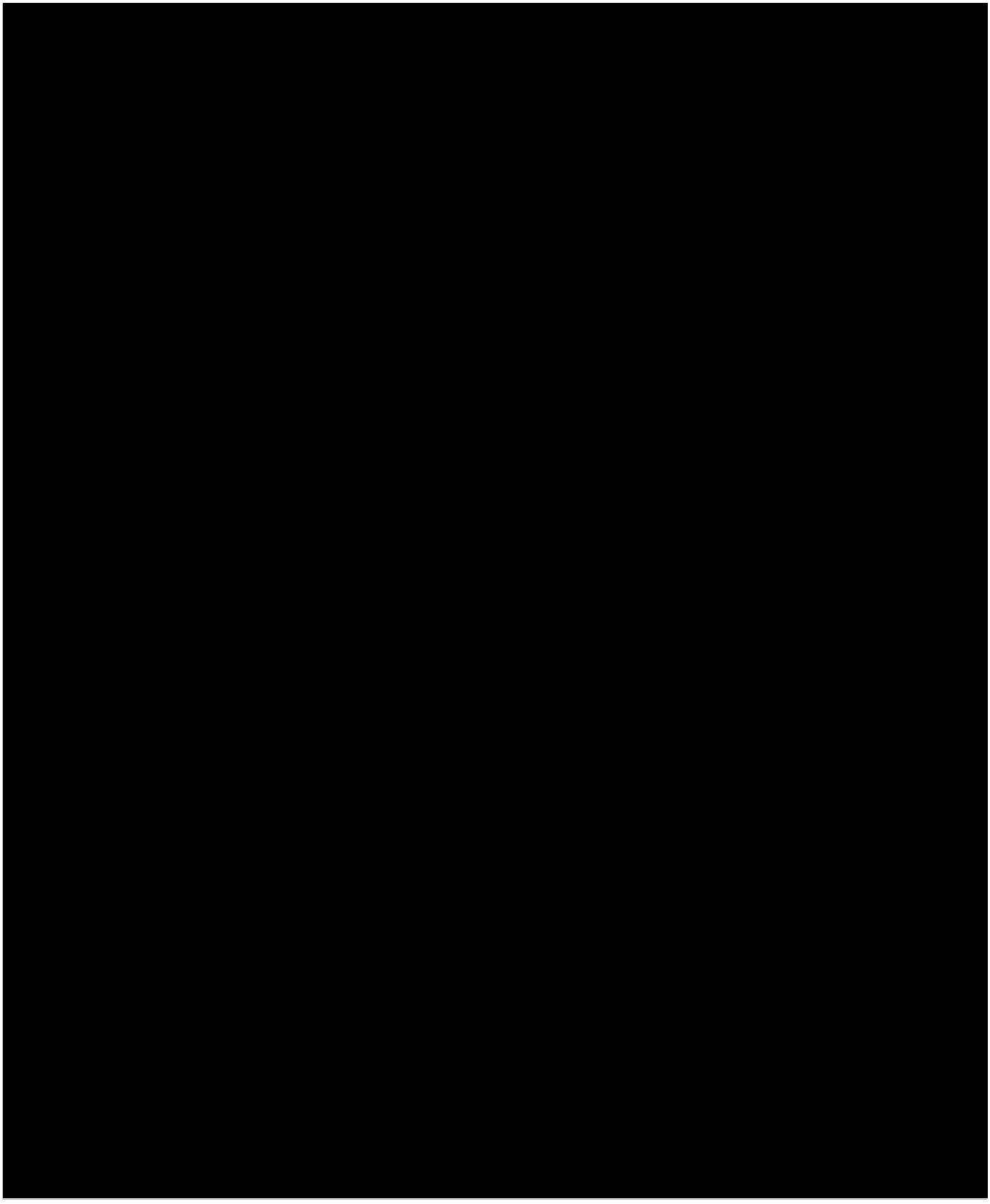
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000580



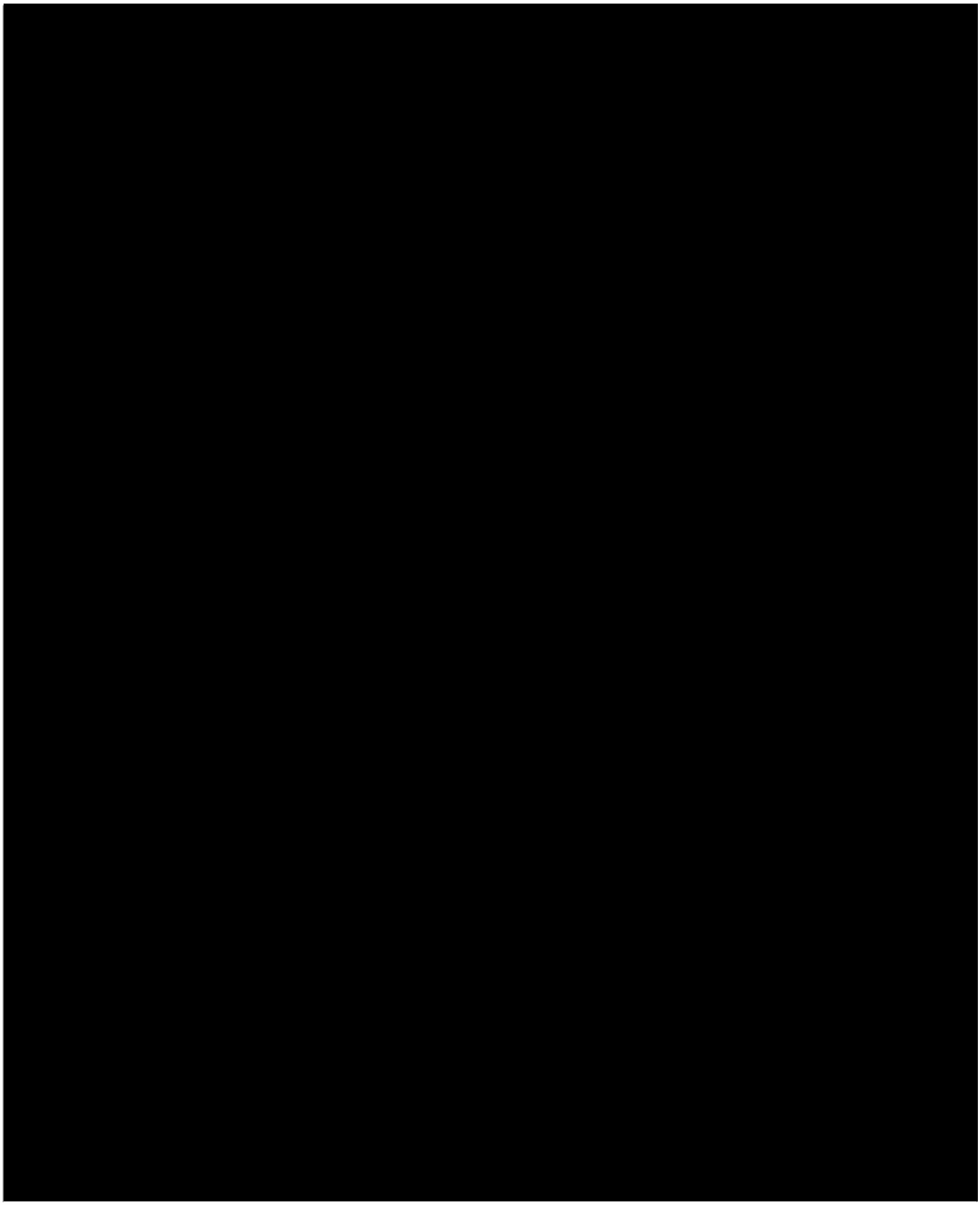
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000581



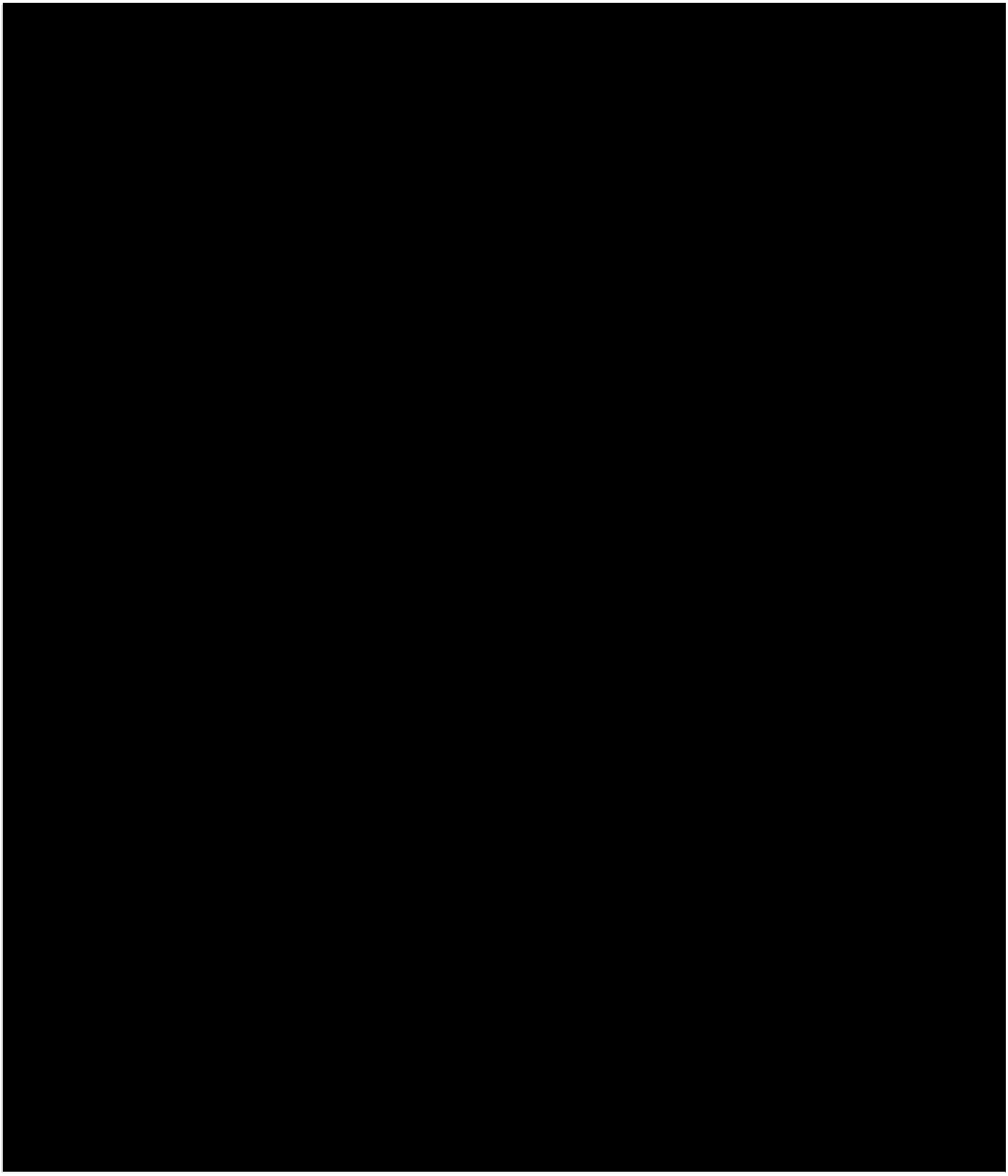
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000582



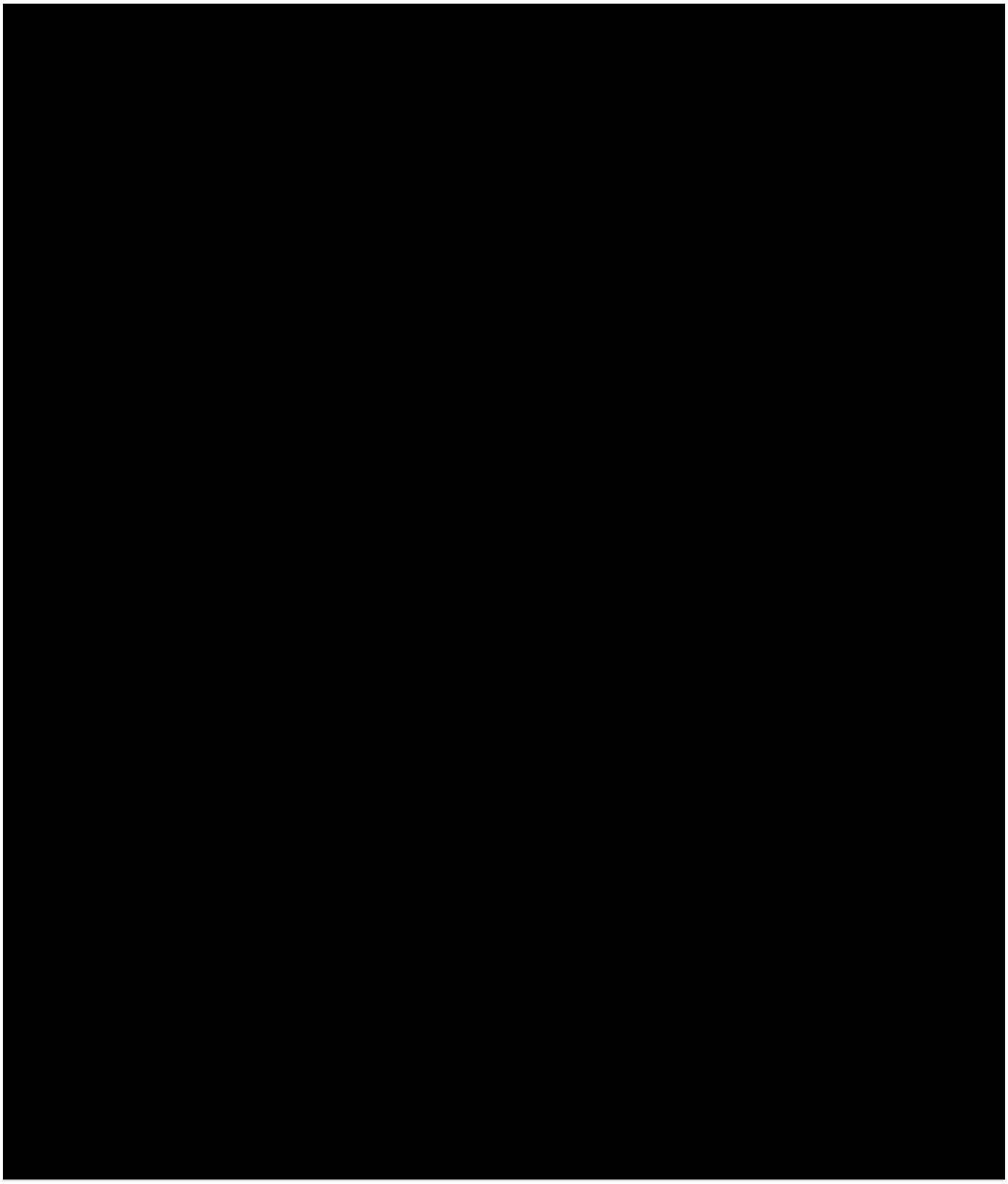
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000583



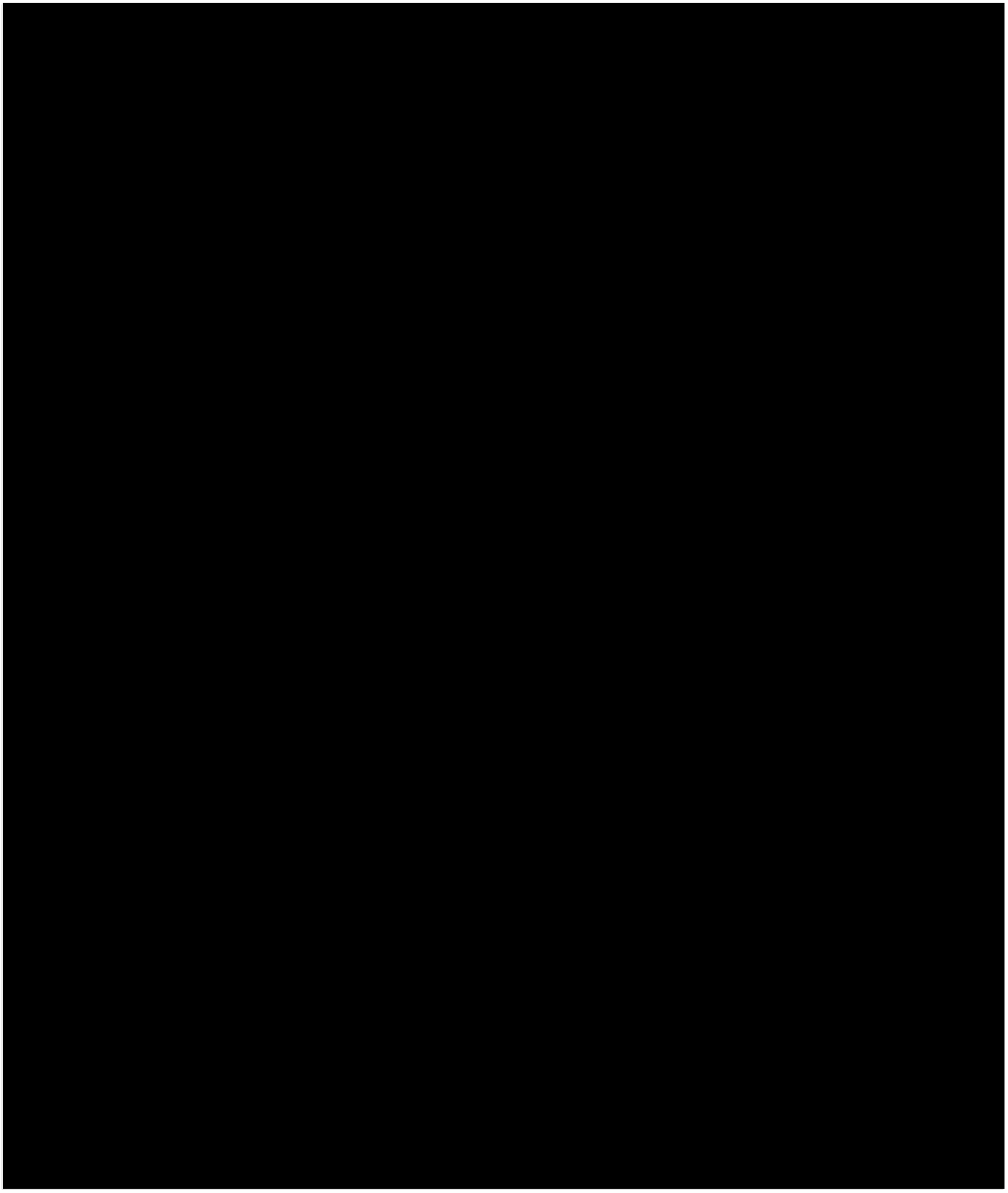
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000584



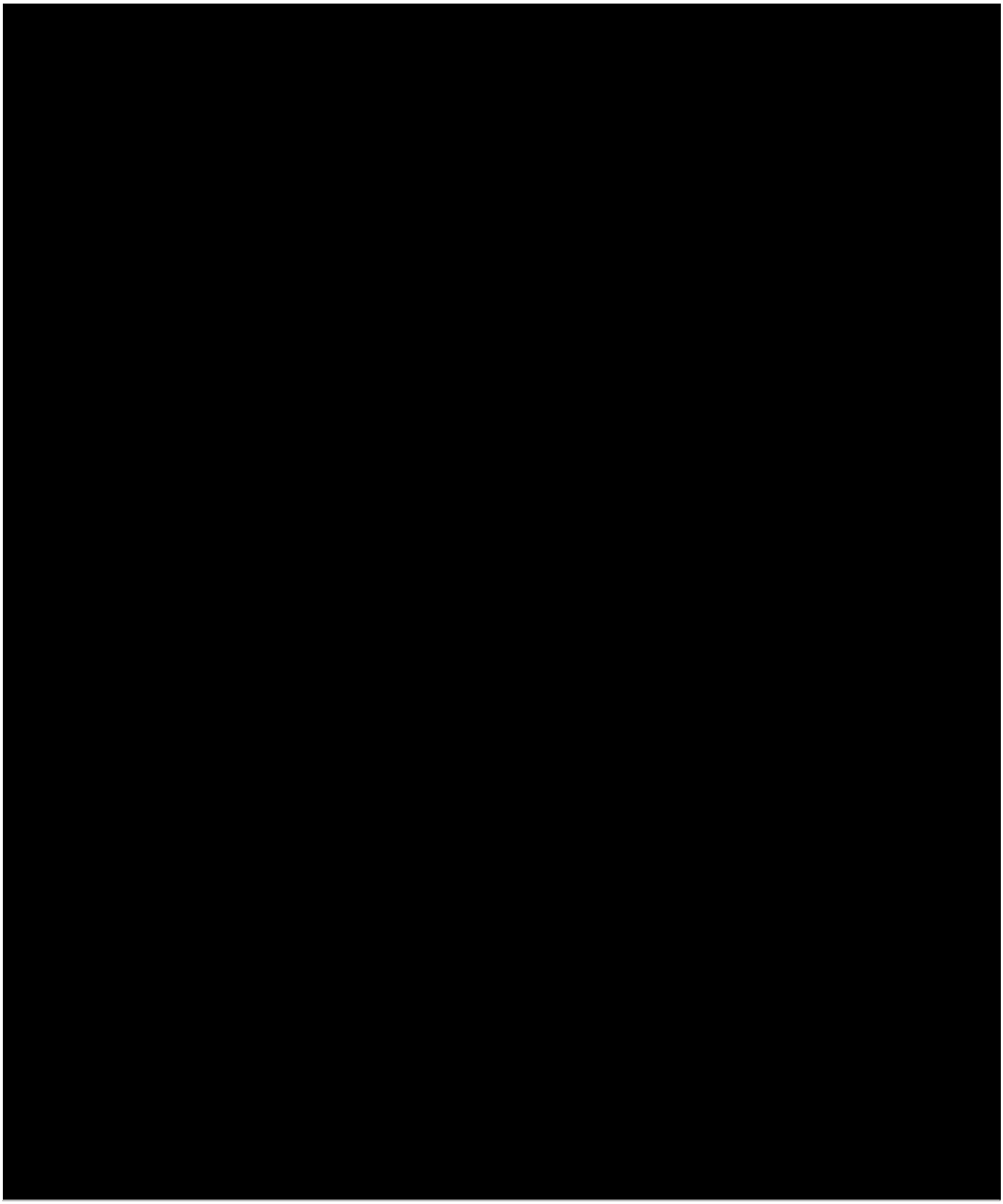
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000585



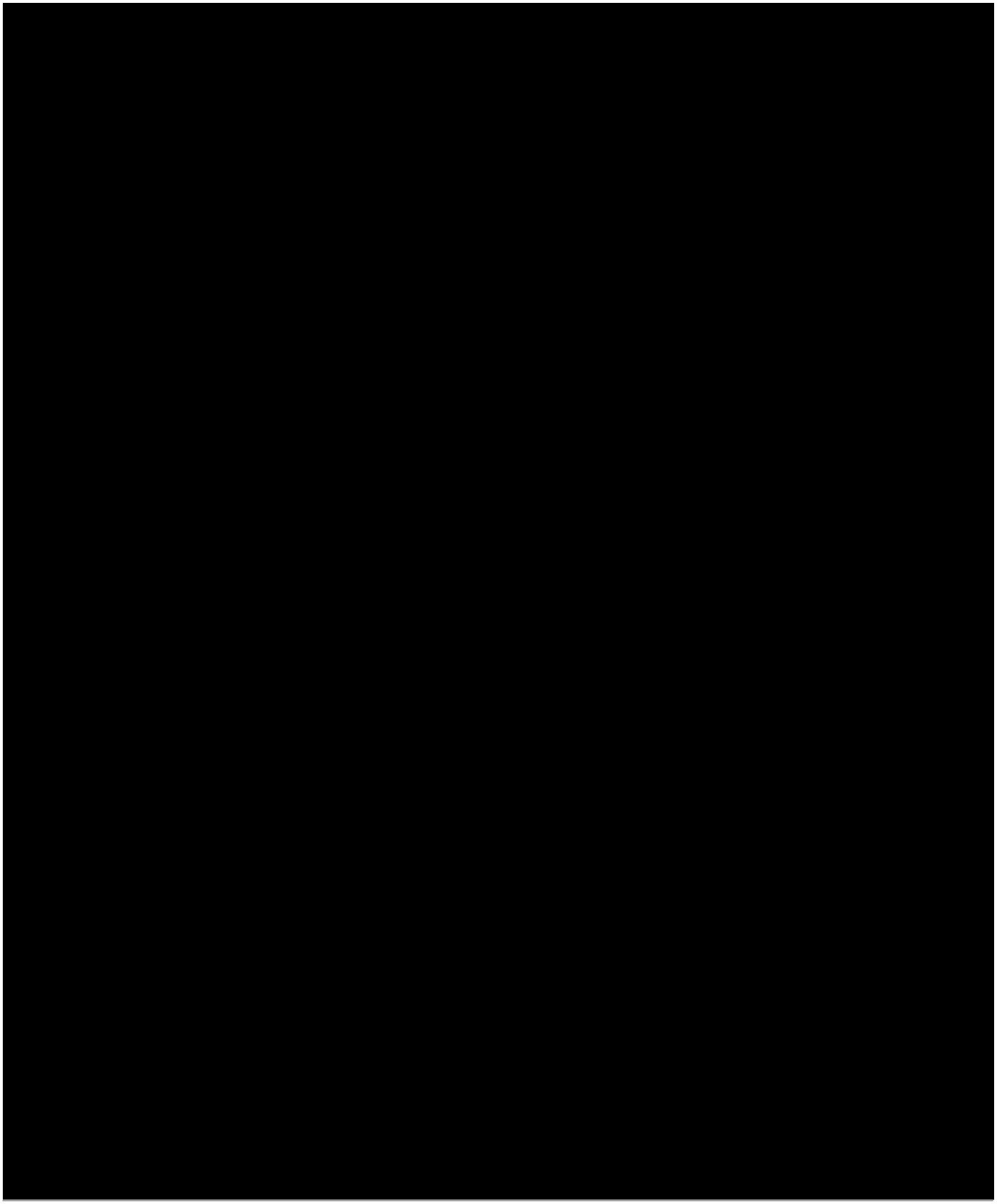
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000586



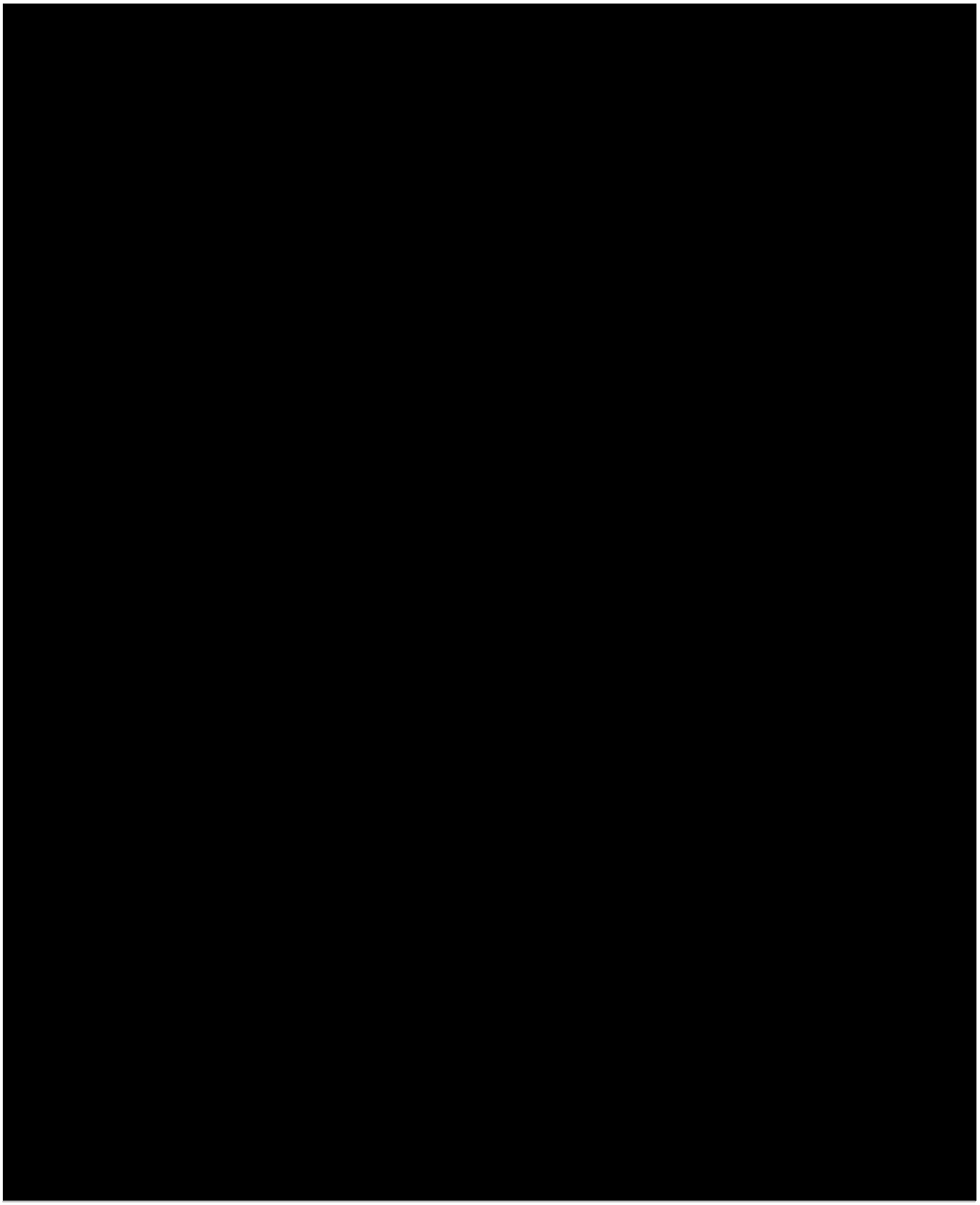
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000587



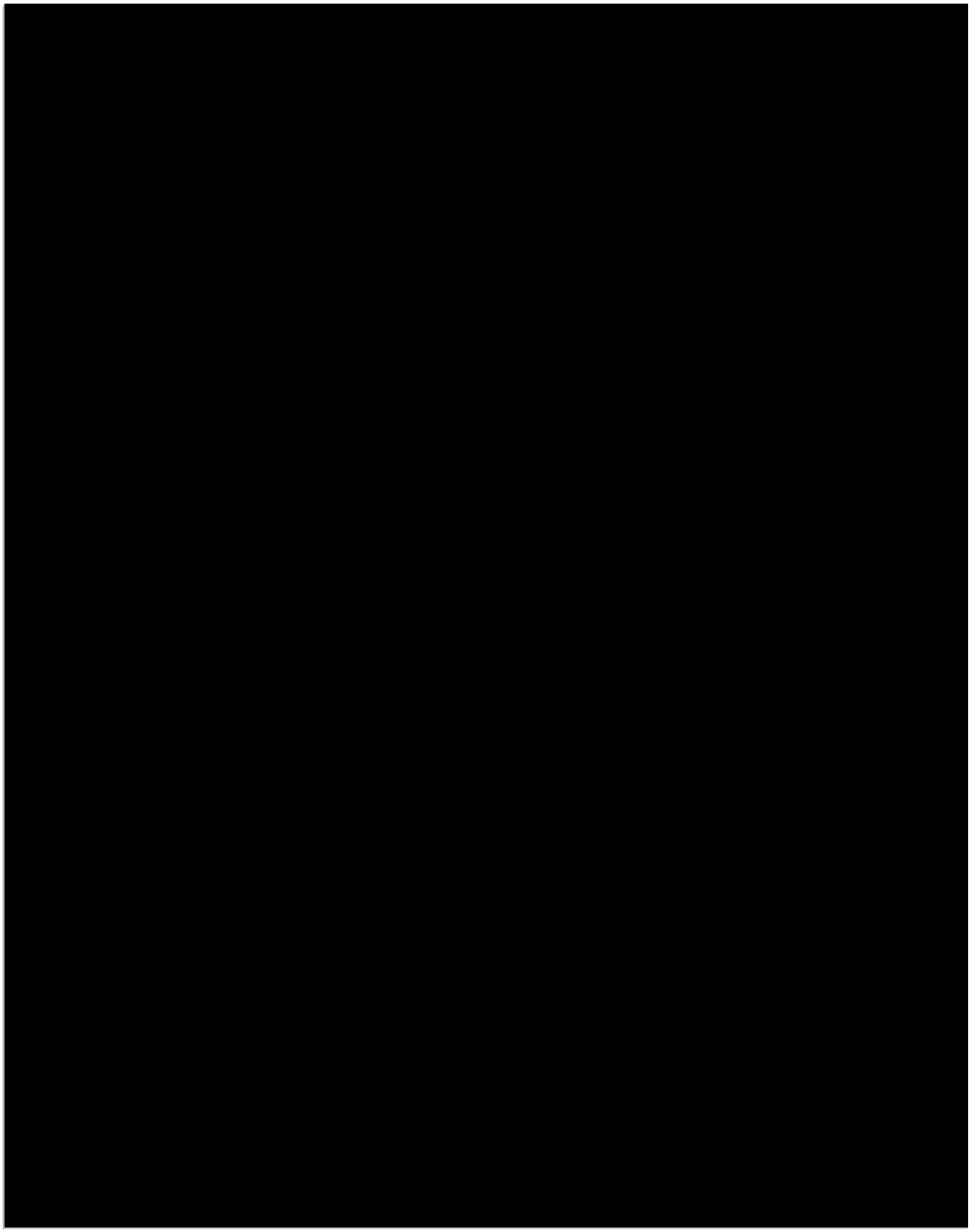
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000588



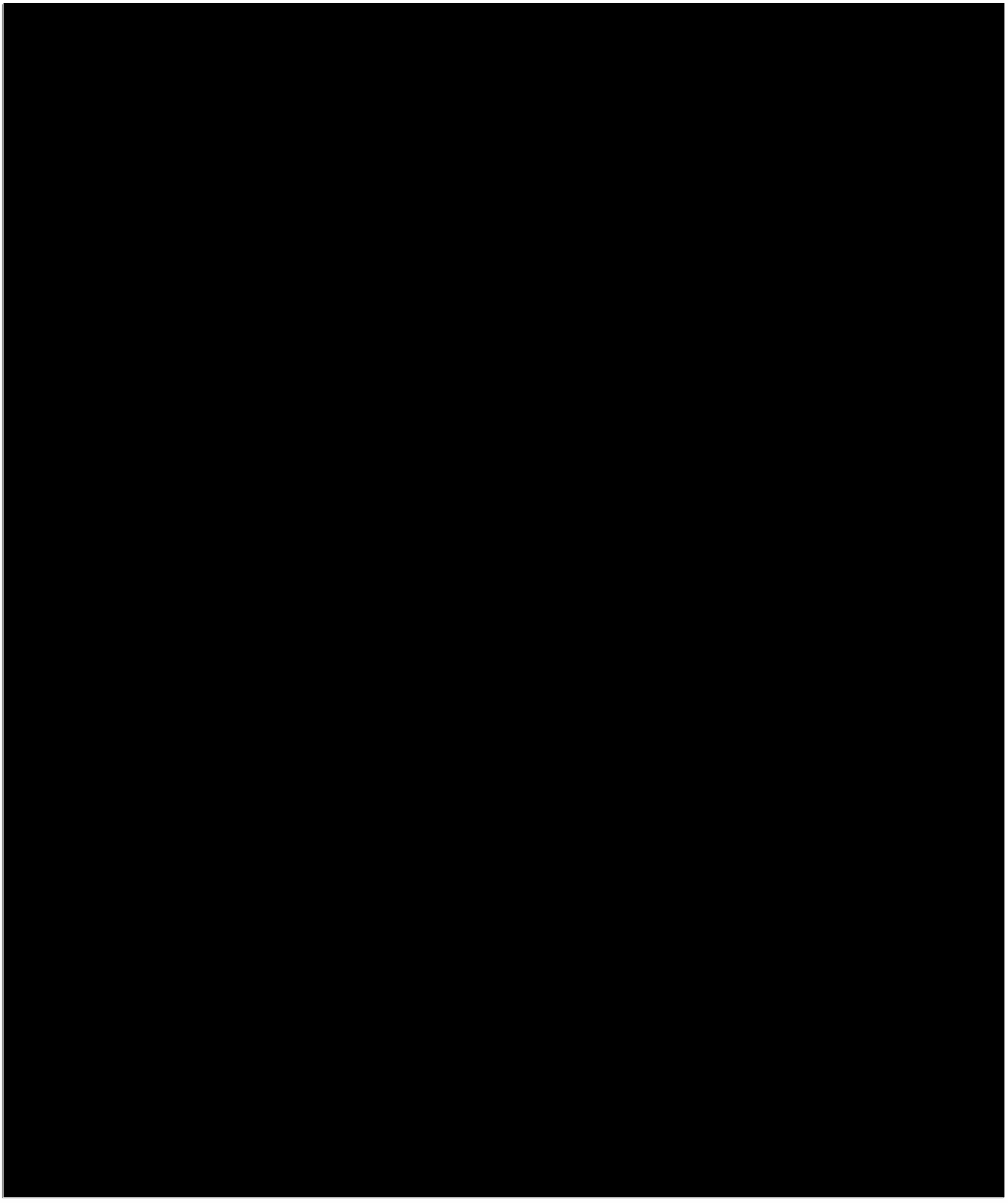
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000589



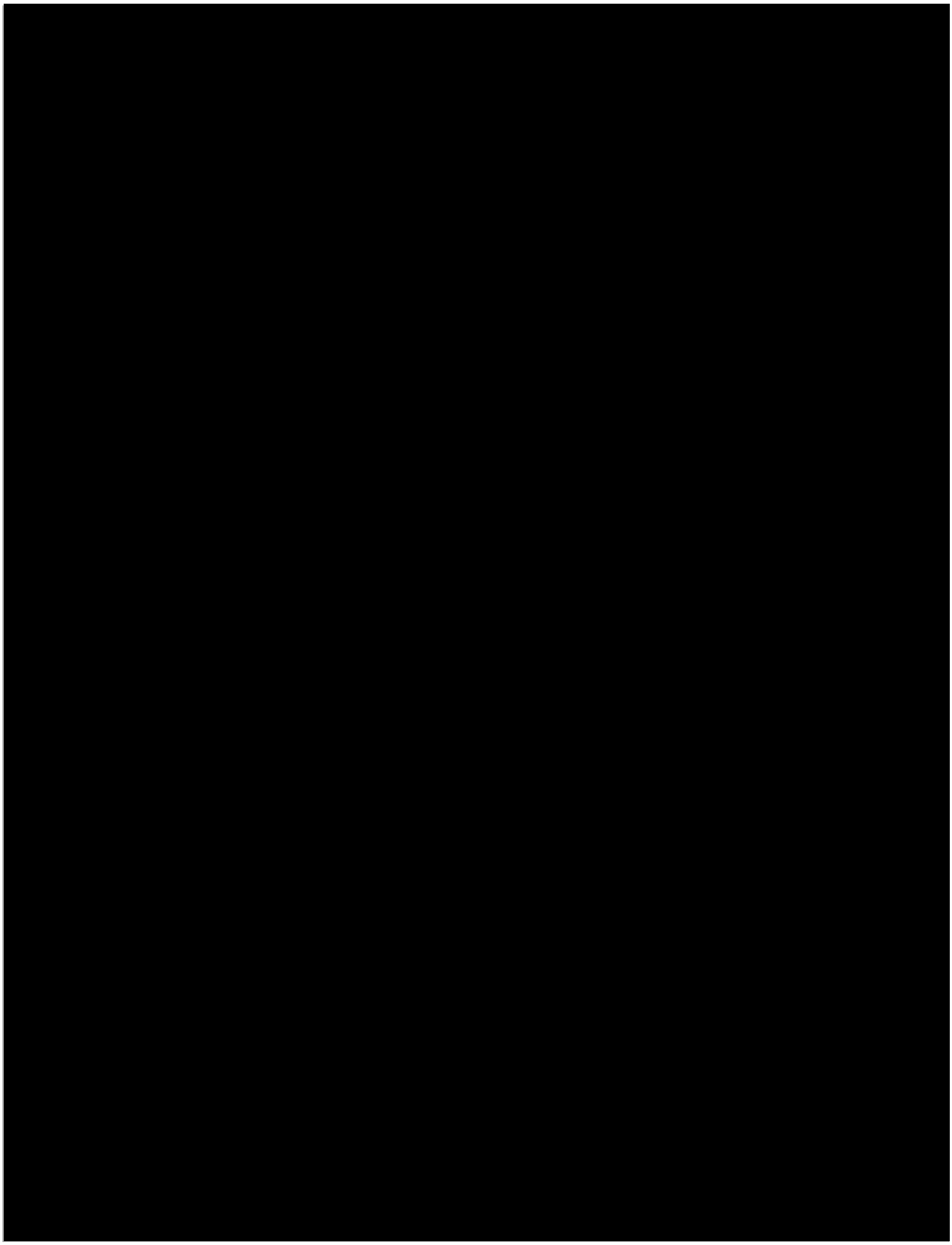
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000590



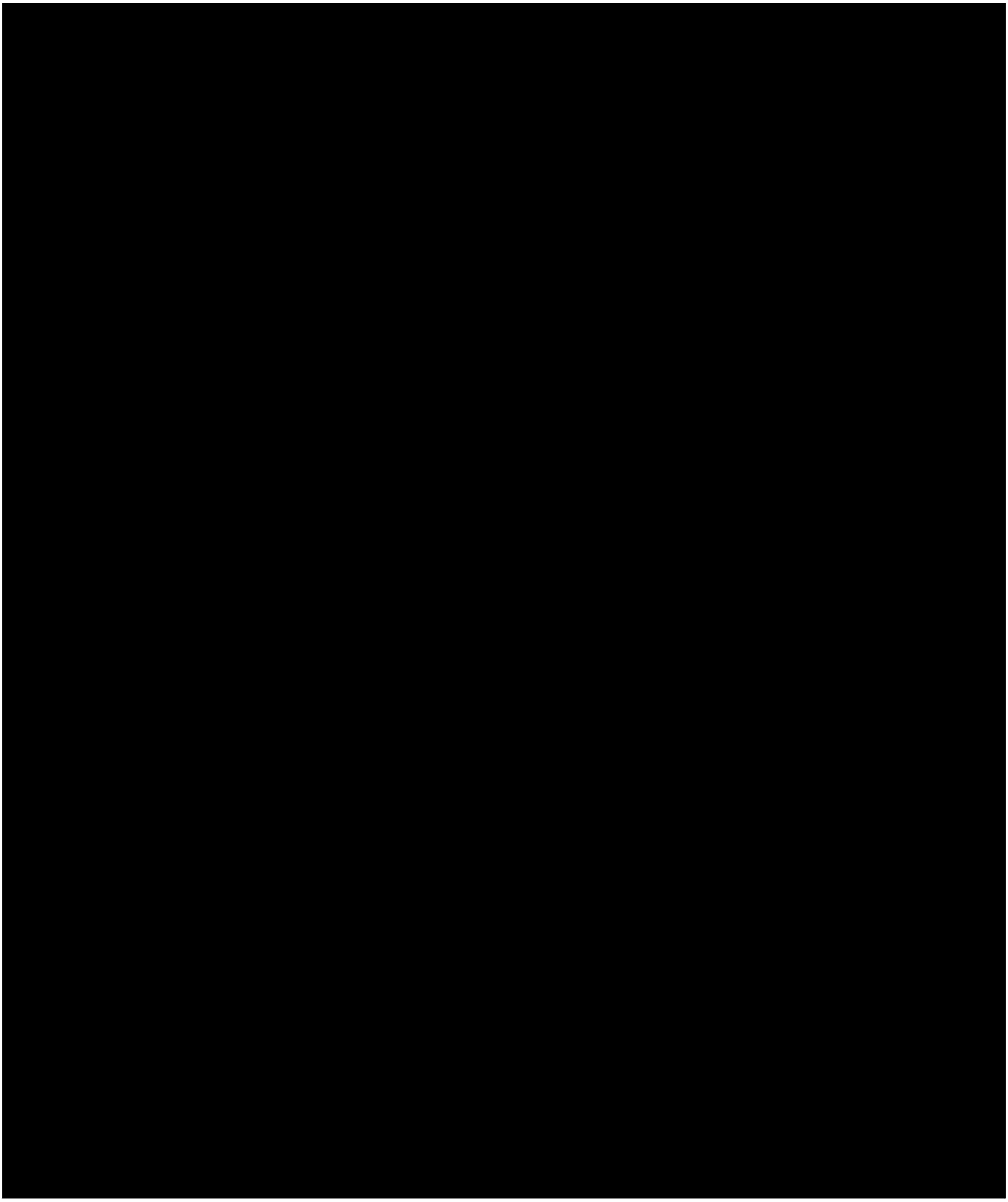
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000591



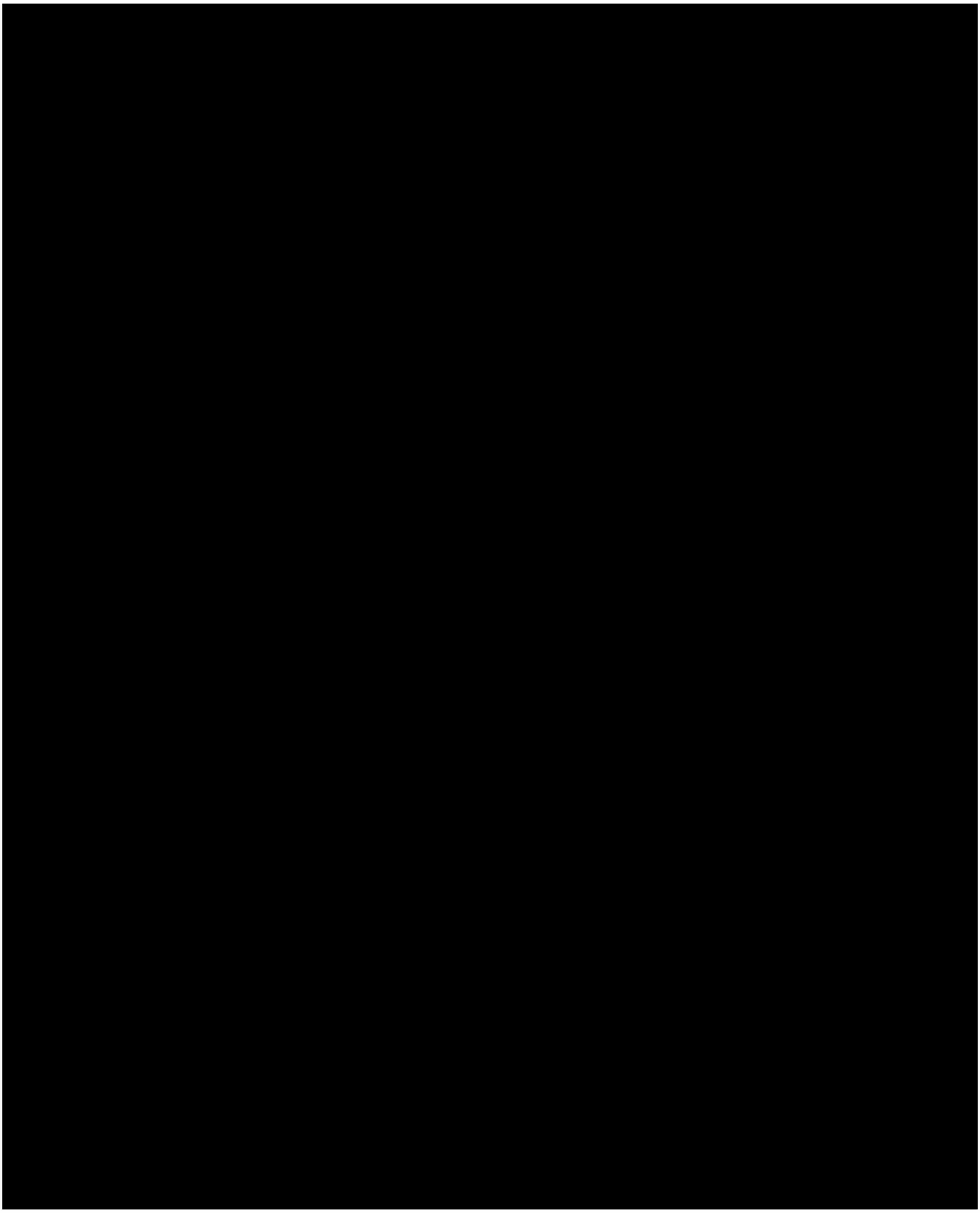
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000592



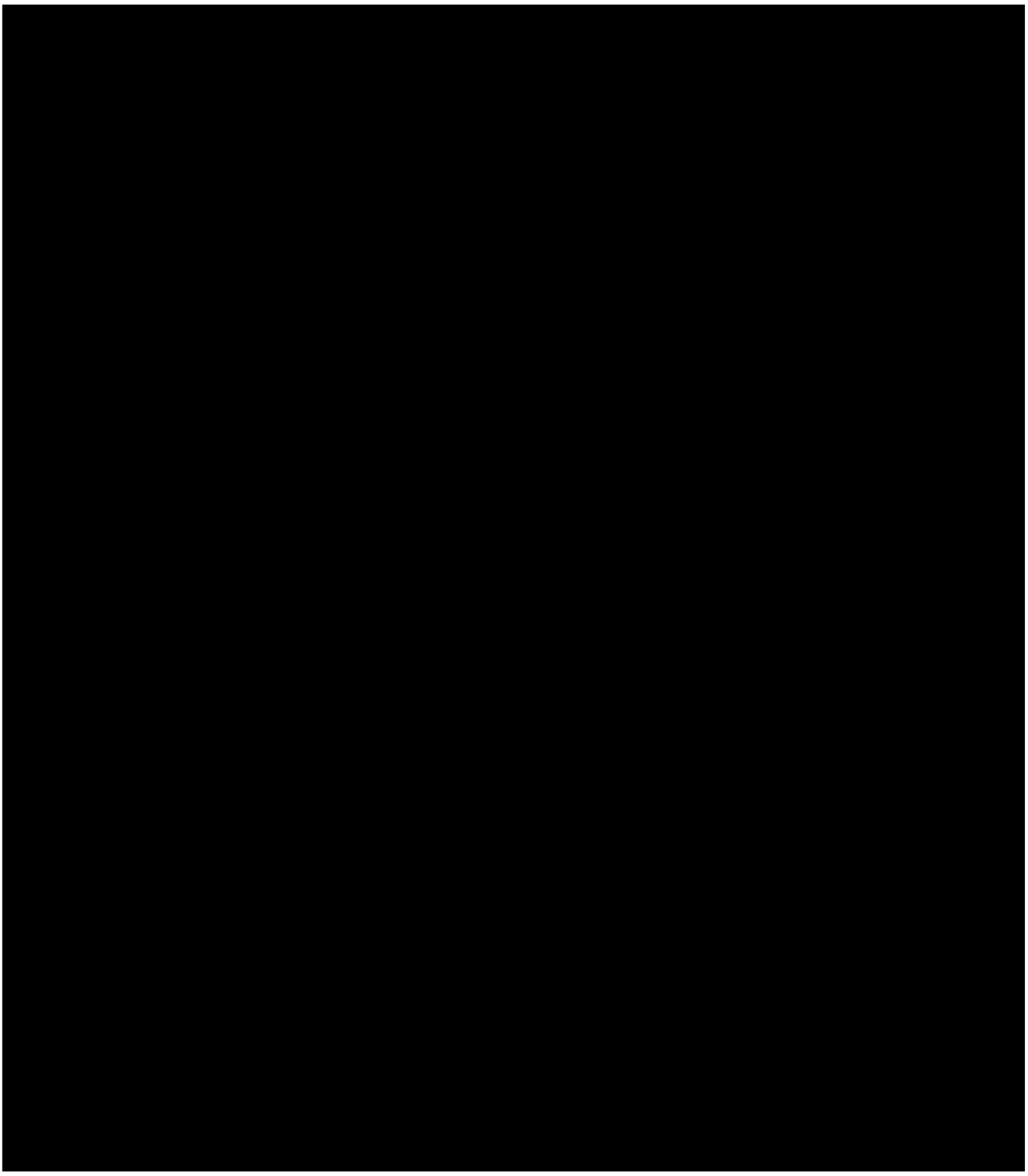
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000593



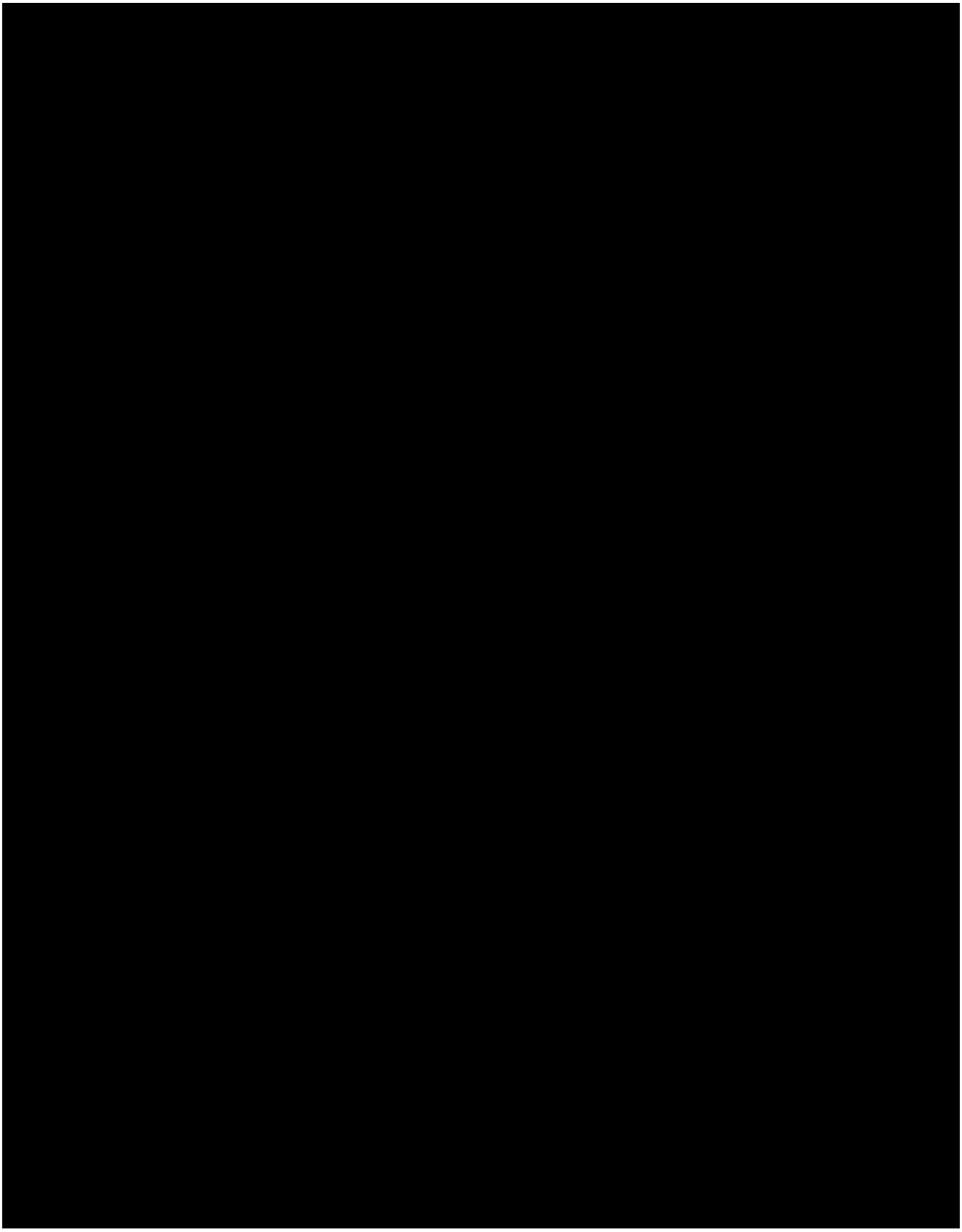
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000594



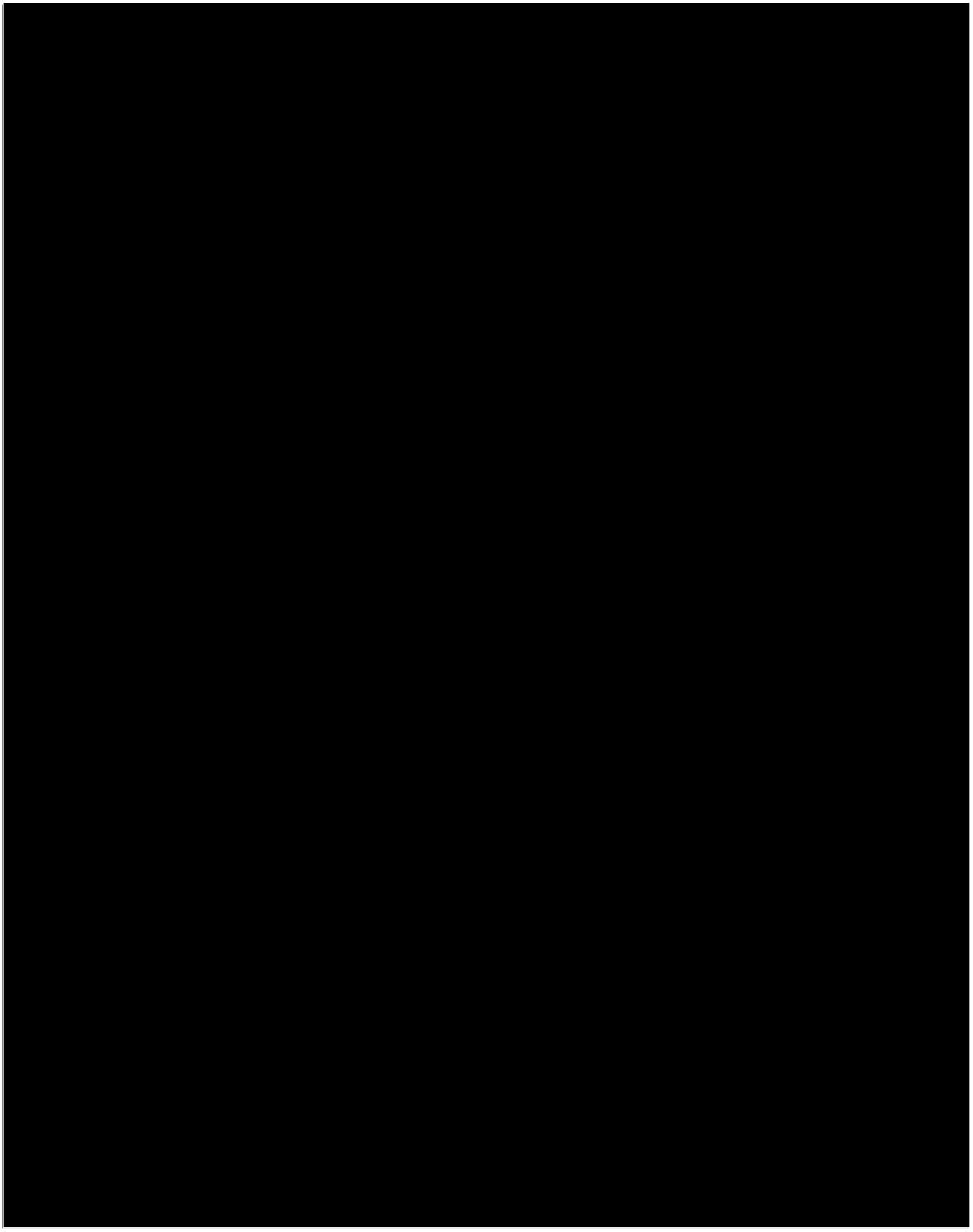
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000595



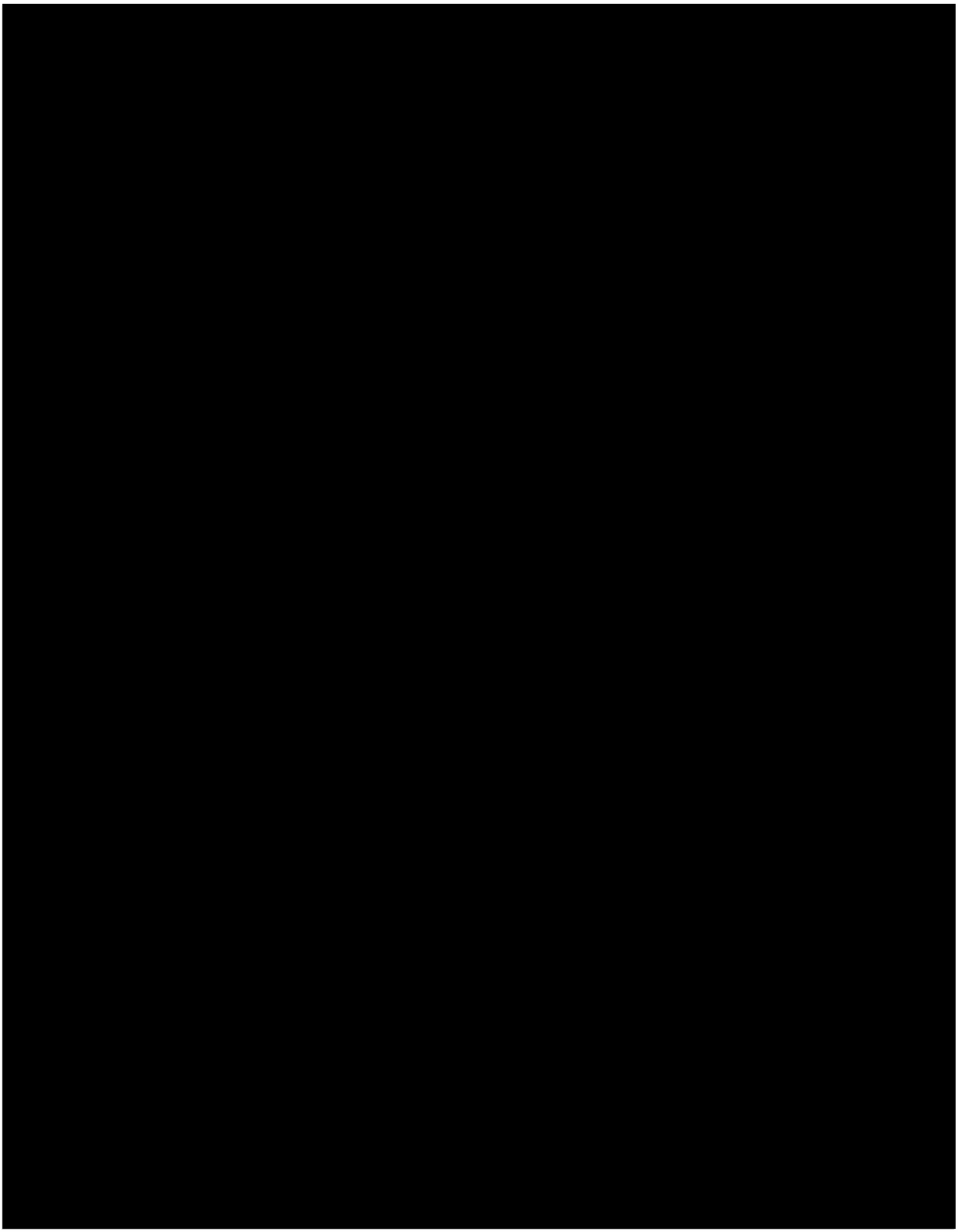
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000596



CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000597



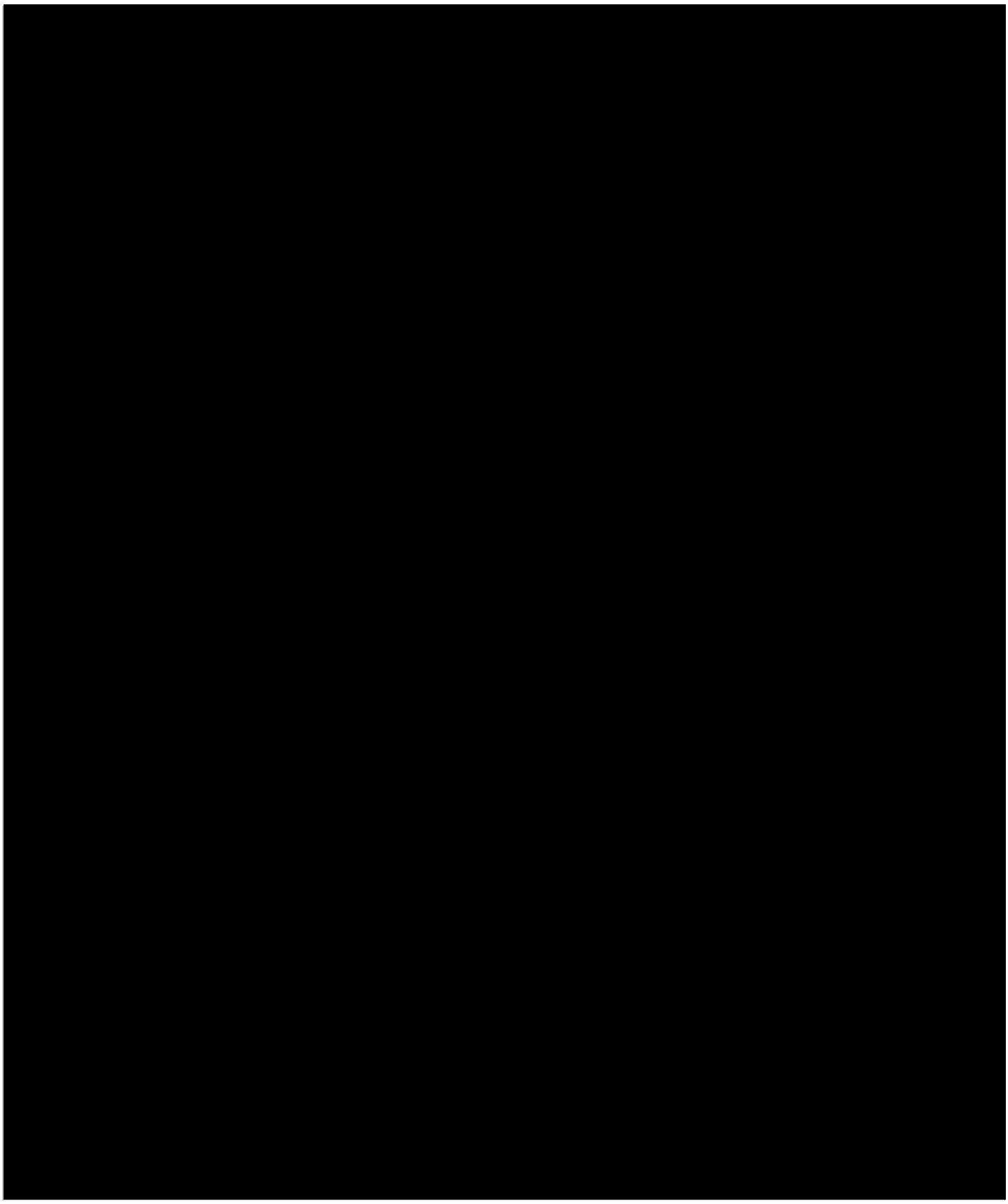
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000598



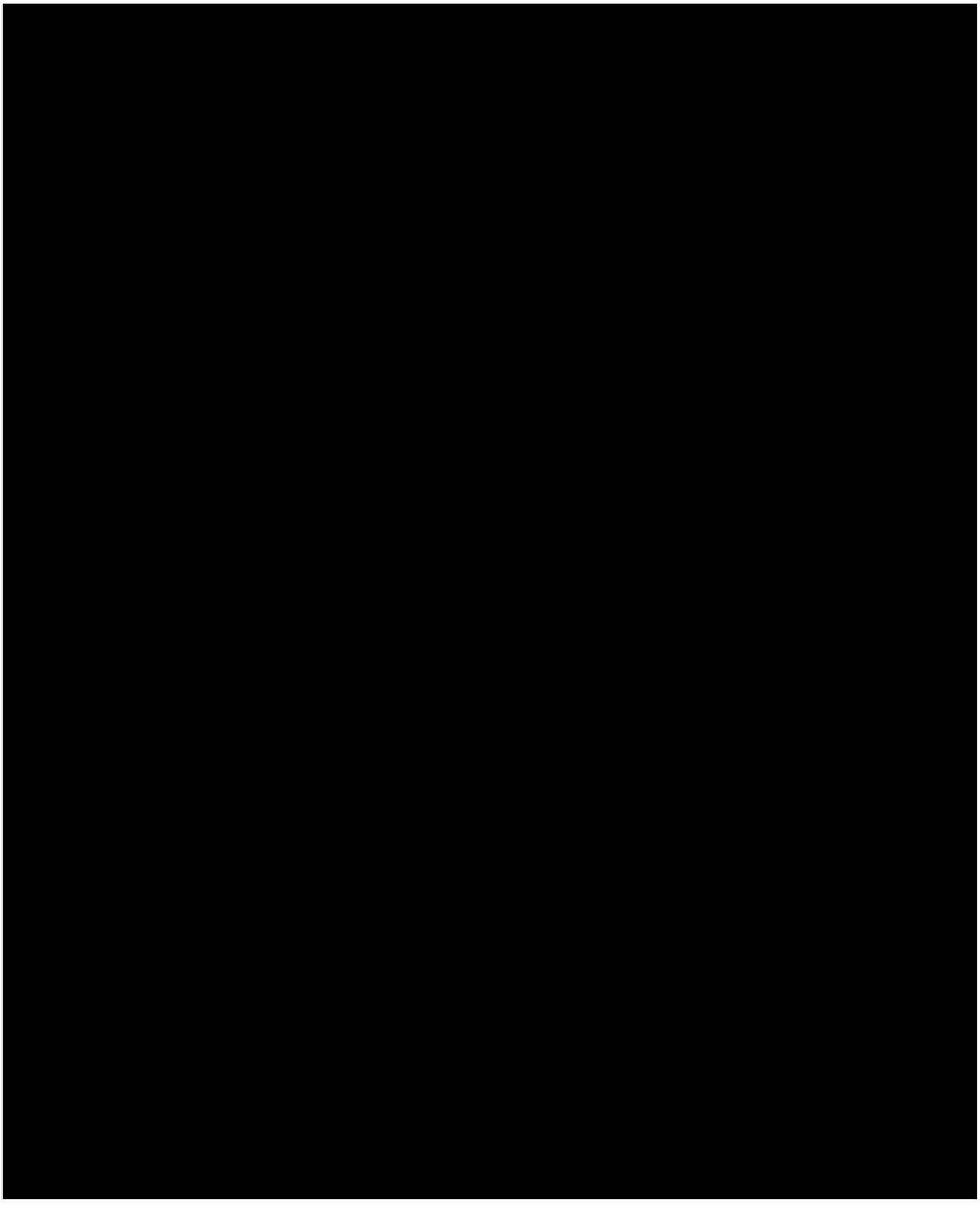
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000599

DRAFT

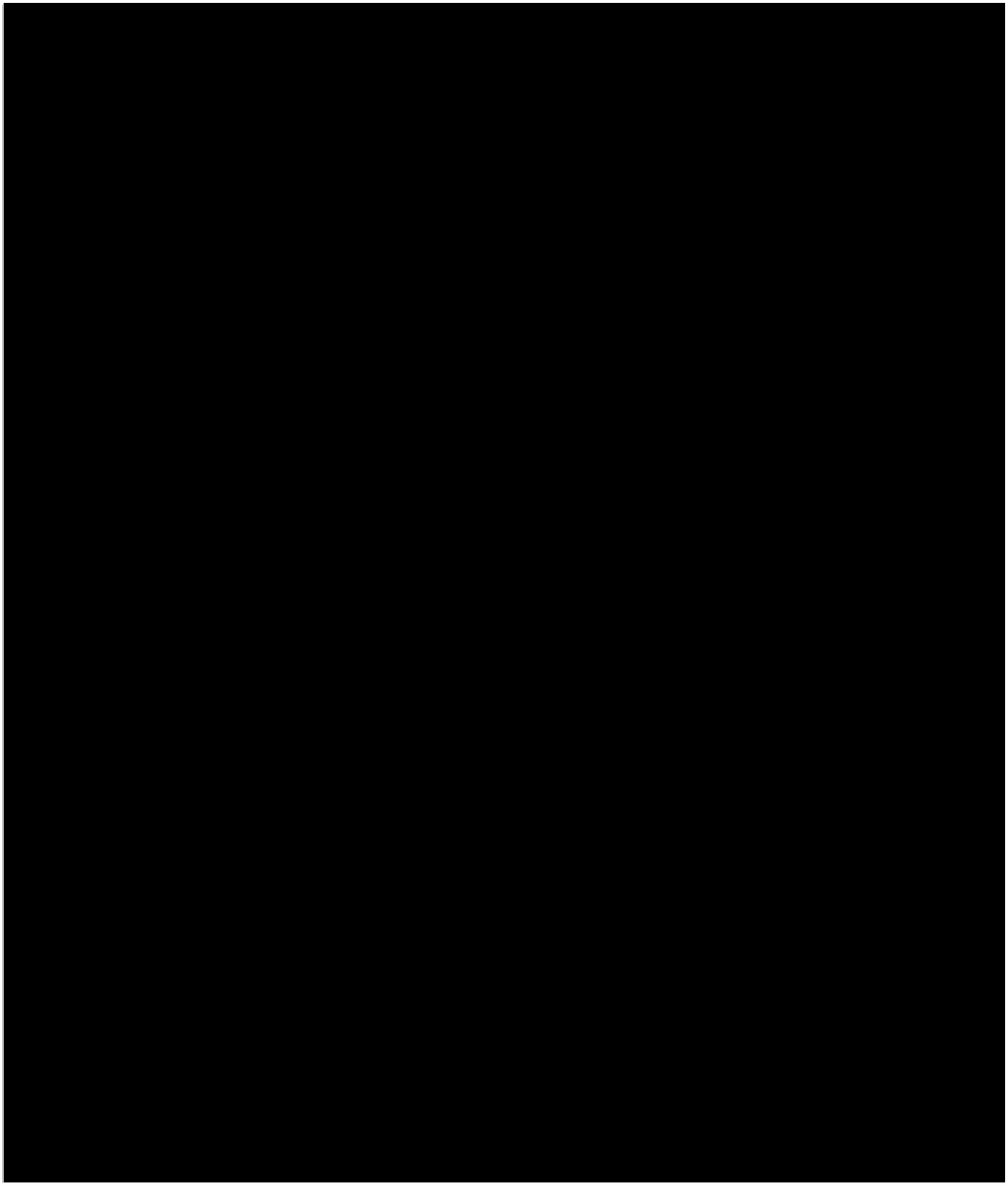
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000600



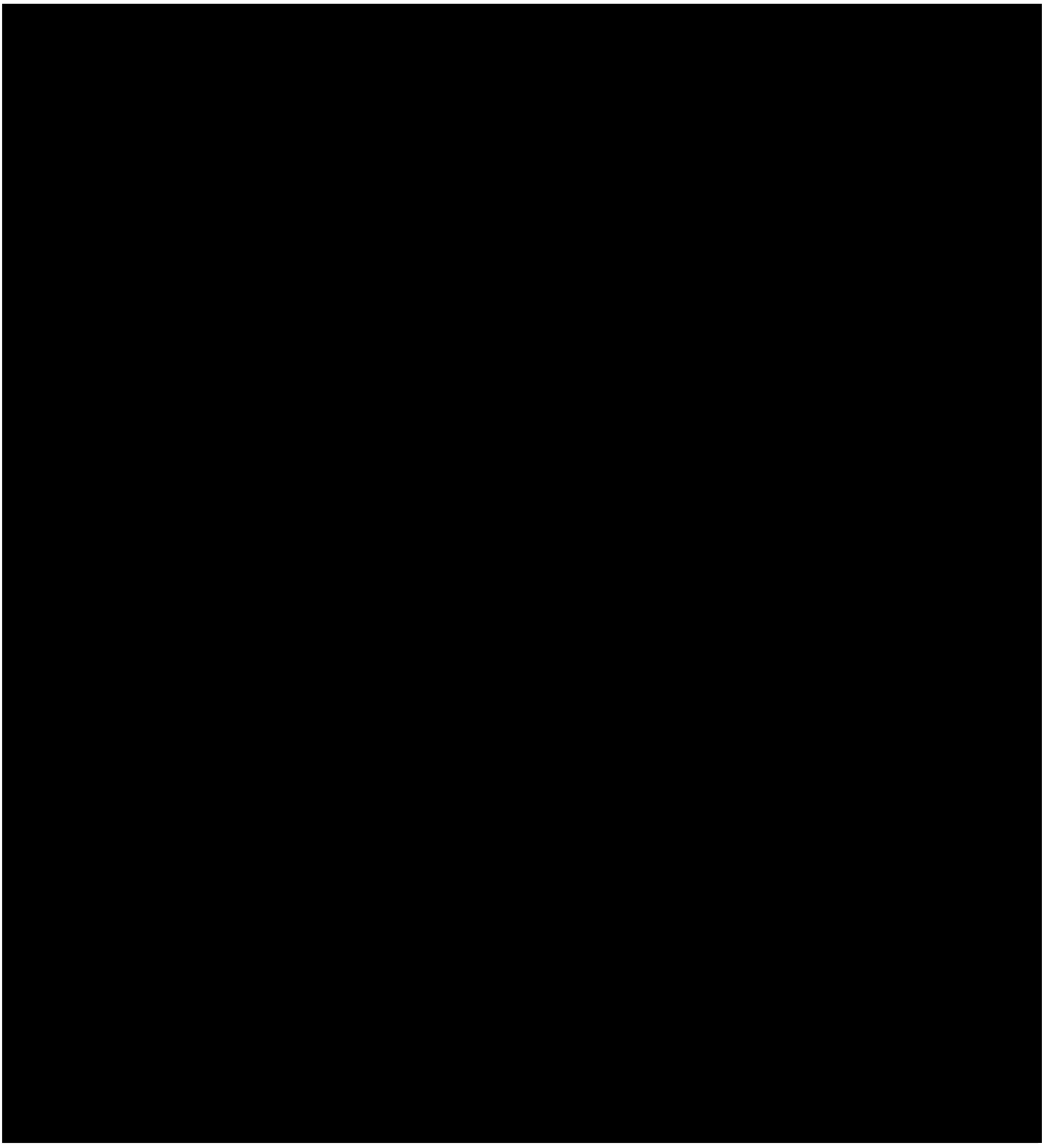
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000601



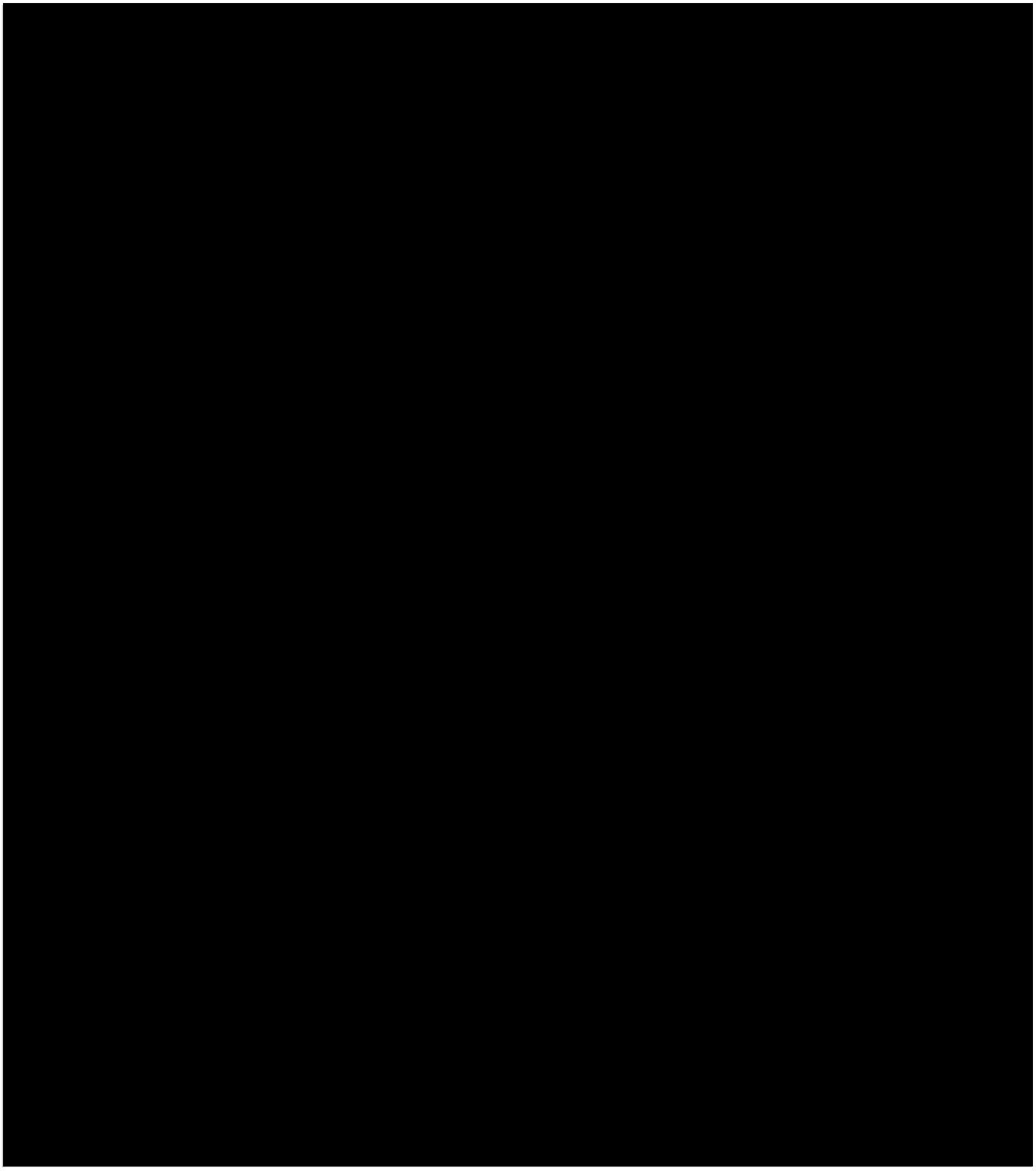
CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000602



CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000603



CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000604



CONFIDENTIAL TREATMENT REQUESTED BY EQUIFAX INC EFXCONG-EC000000605