

**KESSLER TOPAZ MELTZER
& CHECK, LLP**

JENNIFER L. JOOST (Bar No. 296164)
(jjoost@ktmc.com)
STACEY M. KAPLAN (Bar No. 241989)
(skaplan@ktmc.com)
One Sansome Street, Suite 1850
San Francisco, CA 94104
Tel: (415) 400-3000
Fax: (415) 400-3001

*Counsel for Class Representative SEB Investment
Management AB and Class Counsel*

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

SEB INVESTMENT MANAGEMENT AB, and
WEST PALM BEACH FIREFIGHTERS'
PENSION FUND, Individually and On Behalf of
All Others Similarly Situated,

Plaintiffs,

v.

WELLS FARGO & COMPANY, CHARLES W.
SCHARF, KLEBER R. SANTOS, and CARLY
SANCHEZ,

Defendants.

Case No. 3:22-cv-03811-TLT

**RESPONSE TO THE COURT'S
SUPPLEMENTAL QUESTIONS FOR
THE HEARING**

1 Class Representatives SEB Investment Management AB and West Palm Beach Firefighters'
2 Pension Fund respectfully submit the following declarations in response to the Court's Supplemental
3 Questions for the Hearing issued on April 28, 2026 (Dkt. No. 276): (i) the Declaration of Eric A. Nordskog
4 in Response to the Court's Supplemental Questions for the Hearing (attached as Exhibit A); and (ii) the
5 Declaration of Sharan Nirmul in Response to the Court's Supplemental Questions for the Hearing (attached
6 as Exhibit B).

7 Dated: April 30, 2026

Respectfully submitted,

8 **KESSLER TOPAZ MELTZER**
9 **& CHECK, LLP**

10 /s/ Sharan Nirmul

SHARAN NIRMUL*

(snirmul@ktmc.com)

JOSHUA A. MATERESE*

(jmaterese@ktmc.com)

EVAN R. HOEY*

(ehoey@ktmc.com)

MARIANNE UY*

(muy@ktmc.com)

280 King of Prussia Road

Radnor, PA 19087

Tel: (610) 667-7706

Fax: (610) 667-7056

17 -and-

19 JENNIFER L. JOOST (Bar No. 296164)

(jjoost@ktmc.com)

20 STACEY M. KAPLAN (Bar No. 241989)

(skaplan@ktmc.com)

21 One Sansome Street, Suite 1850

San Francisco, CA 94104

Tel: (415) 400-3000

Fax: (415) 400-3001

24 *Counsel for Class Representative SEB Investment*
25 *Management AB and Class Counsel*

26 **SAXENA WHITE P.A.**

DAVID R. KAPLAN (SBN 230144)

(dkaplan@saxenawhite.com)

27 EMILY R. BISHOP (SBN 319383)

28 (ebishop@saxenawhite.com)

1 505 Lomas Santa Fe Dr.
2 Suite #180
3 Solana Beach, CA 92075
4 Tel: (858) 997-0860
5 Fax: (858) 369-0096

6 -and-

7 LESTER R. HOOKER (SBN 241590)
8 (lhooker@saxenawhite.com)
9 DIANNE M. PITRE (SBN 286199)
10 (dpitre@saxenawhite.com)
11 7777 Glades Road, Suite 300
12 Boca Raton, FL 33434
13 Tel: (561) 394-3399
14 Fax: (561) 394-3382

15 *Counsel for Class Representative West Palm Beach*
16 *Firefighters' Pension Fund*

17 **KLAUSNER KAUFMAN JENSEN & LEVINSON**
18 **ROBERT D. KLAUSNER***
19 (bob@robertdklausner.com)
20 **BONNI S. JENSEN***
21 (bonni@robertdklausner.com)
22 7080 Northwest 4th Street
23 Plantation, FL 33317
24 Tel: (954) 916-1202
25 Fax: (954) 916-1232

26 *Fiduciary Counsel for Class Representative West Palm*
27 *Beach Firefighters' Pension Fund*

28 *appearance *pro hac vice*

EXHIBIT A

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

SEB INVESTMENT MANAGEMENT AB, and
WEST PALM BEACH FIREFIGHTERS'
PENSION FUND, Individually and on Behalf of
All Others Similarly Situated,

Plaintiffs,

v.

WELLS FARGO & COMPANY, CHARLES W.
SCHARF, KLEBER R. SANTOS, and CARLY
SANCHEZ,

Defendants.

Case No. 22-cv-03811-TLT

**DECLARATION OF ERIC A.
NORDSKOG IN RESPONSE TO THE
COURT'S SUPPLEMENTAL
QUESTIONS FOR THE HEARING**

1 I, Eric A. Nordskog, declare as follows:

2 1. I am a Director at A.B. Data, Ltd.’s Class Action Administration Company
3 (“A.B. Data”), whose Corporate Office is located in Milwaukee, Wisconsin. A.B. Data serves as
4 the Claims Administrator for the proposed settlement (“Settlement”) of the above-captioned
5 securities class action (“Action”). I submit this declaration in response to the Court’s request for
6 additional information related to the administration of the Settlement (“Supplemental Questions”)
7 (Dkt. No. 276).

8 **FINANCIAL DISCLOSURES AND REVENUE SHARING**

9 2. A.B. Data will not receive any additional revenue, money, or thing of value in
10 connection with the settlement beyond the fees and expenses that were described in connection
11 with the preliminary approval papers. *See, e.g.*, Declaration of Eric A. Nordskog Regarding A.B.
12 Data Ltd.’s Notice and Administration Costs dated November 3, 2025 (Dkt. No. 268-1). I can also
13 confirm that A.B. Data does not have any financial arrangements with any third parties that relate
14 to the administration of the Settlement (including, interest or float on settlement deposits, payments
15 from depository banks, and any revenue-sharing, ownership percentage, or markups on settlement
16 services from payment, claims processing, social media, or other vendors). *See also* Declaration
17 of Eric A. Nordskog in Support of Plaintiffs’ Unopposed Motion for Preliminary Approval of
18 Settlement dated October 15, 2025 (“Notice Plan Declaration”) (Dkt. No. 254-3) (“A.B. Data will
19 not receive any additional revenue beyond what is detailed in its proposal. A.B. Data also confirms
20 that it does not have any financial arrangements with any third parties that are related to the
21 administration of the Settlement.”).

22 **FEES AND RESIDUALS**

23 3. A.B. Data and its subcontractors will not charge any fees to Class Members or
24 claimants in connection with the Settlement, including interchange fees, dormancy fees, or the
25
26
27
28

1 retention of residual balances.¹ All payments to eligible Class Members will be made via check or
2 wire transfer. There will be no fees associated with these transactions.

3 **DATA PRIVACY**

4 4. A.B. Data is committed to protecting the confidentiality, integrity, and availability
5 of personal identifying information and other information it collects from Class Members. A.B.
6 Data confirms that data about visitors to the Settlement website and all other Class Member data
7 provided in connection with the Settlement has been used and will continue to be used only for the
8 purposes of claims processing and administering the Settlement. A.B. Data further confirms that
9 data about visitors to the Settlement website and all other Class Member data will not be shared
10 with third parties not involved with administering the Settlement, including via trackers or pixels.

11 5. A.B. Data has numerous control systems and procedures in place to ensure the
12 secure handling of Class Member data, which A.B. Data believes meet or exceed relevant industry
13 standards. A summary of those systems and procedures, addressing the items highlighted in the
14 Northern District of California's *Procedural Guidance for Class Action Settlements* (including
15 technical, administrative, and physical controls; retention; destruction; audits; and crisis response;
16 etc.) was previously submitted with the Notice Plan Declaration (*see* Dkt. No. 254-3, Ex. B) and
17 is attached hereto as Exhibit A.

18 6. Further, A.B. Data has a number of high-profile clients, including the Securities
19 and Exchange Commission, the United States Department of Justice, the Attorneys General of
20 nearly all 50 states, other agencies of the United States government, and the Government of Israel,
21 as well as direct banking and payment services companies with some of the most recognized
22 brands in United States financial services and some of the largest credit card issuers in the world.
23 As a result, A.B. Data is frequently subjected to physical, logical, data, and information systems
24 security reviews and audits. A.B. Data continues to be compliant with its clients' security standards

25 _____
26 ¹ Interchange fees, dormancy fees, and the retention of residual balances arise in the context
27 of settlements where payments are made by prepaid credit cards. Here, eligible Class Members do
28 not have the option of receiving their payment by prepaid credit card so these fees are not
applicable.

1 as well as ISO/IEC 27001/2 and Payment Card Industry (PCI) data-security standards, the Gramm-
2 Leach-Bliley Act (GLB) of 1999, the National Association of Insurance Commissioners (NAIC)
3 Regulations, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the
4 Health Information Technology for Economic and Clinical Health Act (HITECH). *See also* Dkt.
5 No. 254-3, Ex. A (copy of A.B. Data resume).

6 7. A.B. Data accepts responsibility for the security of Class Member information and
7 data, including information, data and documents submitted by claimants in connection with the
8 claims process for the Settlement. All data provided to A.B. Data by the Parties to the Action
9 and/or Class Members has been used and will continue to be used solely for the purpose of
10 administering and effecting the Settlement. *See* Notice Plan Declaration, Ex. B (Chart, Row 1).
11 Specifically, Class Members' information and data will not be used, disseminated, or disclosed by
12 or to any other person or entity for any other purpose. A.B. Data has complied with and will
13 continue to comply with the provisions regarding data privacy set forth in this District's
14 *Procedural Guidance for Class Action Settlements*. *See* Chart attached as Exhibit A hereto.

15 **USE OF ARTIFICIAL INTELLIGENCE**

16 8. Neither A.B. Data nor its subcontractors have used or intend to use artificial
17 intelligence in connection with administrating the Settlement, including the processing of Claims.
18 Because the nature of securities class action settlements requires the submission of documentation
19 detailing transactions in eligible securities as well as calculation programs requiring the entry of
20 class members' transactional information in order to calculate losses, A.B. Data continues to rely
21 on humans to review and input transactional information submitted on paper claim forms (as
22 opposed to electronic claim submissions which get scanned and uploaded to A.B. Data's database).
23 In the event A.B. Data determines that the use of artificial intelligence would be useful in some
24 aspect of this administration, A.B. Data will, before utilizing artificial intelligence, confer with
25 Class Counsel and take the necessary steps to ensure the accuracy and lack of bias in its use.

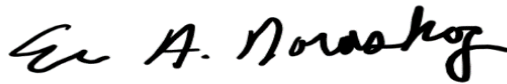
FRAUD PREVENTION

1
2 9. A.B. Data employs a number of techniques to deter illegitimate claim submissions
3 from bad actors, bots, and others attempting to defraud the claims process. A.B. Data also reviews
4 and analyzes various filing patterns across all existing cases and claims in order to detect anything
5 suspicious. In all settlements it administers, including this Settlement, A.B. Data is continually
6 monitoring and technically enhancing the claims submission portal to detect and block fraudulent
7 activity, and submitted claims are continually reviewed and scored to assess whether a claim may
8 have been submitted by a bad actor, non-class member, or submitted through other nefarious
9 means.

10 10. In addition to the foregoing, A.B. Data will also conduct a search of all Claims
11 submitted for the Settlement using its database of known questionable claim filers. This database
12 contains names, addresses, and aliases of individuals or entities that have been investigated by
13 government agencies for questionable claim filings, as well as the names and contact information
14 compiled from previous settlements that A.B. Data has administered where fraudulent claims were
15 received. A.B. Data updates the database on a regular basis. The database for the Settlement will
16 be searched for all individuals identified as questionable claim filers. A.B. Data will perform
17 searches based on name, aliases, address, and city/ZIP code. In addition, all of A.B. Data's claim
18 processors are trained to identify any potentially inauthentic documentation when processing
19 claims, including claims submitted by claimants not previously captured in our database as
20 previously-identified questionable claim filers. Processors are instructed to flag any questionable
21 claims and route them to management for review.

22 11. Suspicious claims will be subject to additional scrutiny, requests for additional
23 documentation, and other proprietary measures to prove the legitimacy of the claims. Suspicious
24 claimants who do not provide the requested additional documentation or information, or fail to
25 otherwise prove the legitimacy of their claim(s), will be subject to rejection and may not be eligible
26 to receive payment(s) from the Net Settlement Fund.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Eric A. Nordskog

EXHIBIT A



Settlement Administration Data Protection Checklist

Category	Control / Question	Response
Limitation on Use of Data	Affirmation that data provided to the administrator for purposes of notice, settlement, or award administration will be used solely for settlement implementation and for no other purpose	All data provided directly to A.B. Data will be used solely for the purpose of effecting the terms of the Settlement. A.B. Data will not use such information or information to be provided by Settlement Class Members for any other purpose than the administration of the Settlement in this Action; specifically the information provided will not be used, disseminated, or disclosed by or to any other person/entity for any other purpose.
Technical Controls	Firewalls and intrusion detection/prevention systems	A.B. Data uses modern next generation firewall systems which include intrusion detection, prevention, and alerting functions. A.B. Data's Information Security Policy requires firewalls be configured for intrusion detection and alerting of incidents to the A.B. Data IT department staff.
Technical Controls	Endpoint detection and response (EDR) systems	A.B. Data uses host based endpoint protection systems which are managed by the A.B. Data IT Department. These protection systems are configured to provide alerting to the IT team for security events who are in turn responsible for responding as required based on incident severity.
Technical Controls	Complex password requirements	A.B. Data requires complex passwords as part of its Information Security Policy. User accounts are required to have a minimum of 12 character passwords with alpha, numeric, and symbols along with upper and lower cases.
Technical Controls	Multi-factor authentication for access to systems and data	A.B. Data Class Action Administration Systems require Multi-Factor Authentication for access to all claims systems and data.
Technical Controls	Malware protection, anti-virus and vulnerability scanning and penetration tests	A.B. Data uses industry leading endpoint protection systems which include Malware, Anti-Virus and host based intrusion protection technologies. A.B. Data utilizes regular vulnerability testing scans on a monthly basis to detect vulnerabilities in its systems on both internal and external networks. These vulnerability scans are performed by a third party and reported back to the A.B. Data IT department for review and remediation as necessary.
Technical Controls	Data encryption (including, "encrypted at rest and in transit," "scrambled in storage," and "cell- or column-level encryption for PII" protocols)	A.B. Data's data encryption standards follow its Information Security Policy requirements such that all data is encrypted at rest on all servers, and, while in transit, must meet encryption standards of AES256 bit or greater.
Technical Controls	"Key management" for access to encrypted databases (e.g., using a hardware security module (HSM) or a key management service (KMS))	A.B. Data utilizes a KMS (Key Management System) for encrypted databases.

Category	Control / Question	Response
Technical Controls	Access only provided on need-to-know basis	A. B. Data Group uses the "Least Privilege" security model, whereby all user accounts are granted no security permissions by default and only given the least level of security permissions necessary to properly complete user assigned work duties as defined by the specific department management.
Administrative Policies	Personnel and support staff risk assessment and management, including pre-hire background checks and screening processes	All employees must pass a pre-employment background check, including a lawful ten-year criminal record review, employment verification, education verification (if required by position), and credit history. In addition, substance testing is a hiring requirement.
Administrative Policies	Personnel and support staff required to enter into non-disclosure and confidentiality agreements	All employees must sign a Confidentiality Agreement ensuring they will recognize their responsibilities in upholding confidential information accessed using data and resources through A.B. Data's networks, databases, and all technology systems. All employees must also sign a Non-Compete, Trade Secret, Proprietary and Confidential Information Non-Disclosure Agreement. This agreement requires the employee to understand, acknowledge, and agree to all the covenants and conditions not to compete and not to disclose proprietary information without consequences for any violation.
Administrative Policies	Access controls to systems and data, including guidance for granting, modifying, and reviewing access rights	A.B. Data access, modifications and removal is authorized by human resources and managed by its IT department. Access permissions are reviewed and approved by management.
Administrative Policies	Information security and privacy policy trainings, including policy review, best practices, and data security	A.B. Data requires annual Security Awareness Trainings of all employees and upon hire. These trainings cover existing and new security policy changes to the organization. The Information Security Policy is reviewed annually by A.B. Data's Security and Compliance team ensuring it is meeting industry best practices and procedures for the industry. Additional security trainings are required for roles that require elevated levels of data access.
Administrative Policies	No remote access to systems for employees	A.B. Data allows certain employees remote access privileges to its systems as required for performance of their job duties. All remote access utilizes two-factor authentication.
Administrative Policies	Exit interviews/confirmation that terminated/departed employees are immediately cut off from access	A.B. Data's termination procedures require all user account access be removed immediately upon termination. A.B. Data's IT Department is required upon receipt of termination notification to disable account and system access (physical and logical) within one (1) hour, 24 hours per day, 7 days per week.
Administrative Policies	Robust audits of data privacy policies by third-party vendors	A.B. Data currently holds SOC1 SSAE18 annual audit by third part auditors who review its policies annually. Additionally, A.B. Data is currently in the process of obtaining a SOC2 audit report in 2023.
Administrative Policies	Accreditation in accordance with ISO 27001 and SOC2 (among the industry standards listed below)	A.B. Data currently holds SOC1 SSAE18 annual audit by third part auditors who review its policies annually. Additionally, A.B. Data is currently in the process of obtaining a SOC2 audit report in 2023.

Category	Control / Question	Response
Administrative Policies	Disclosure of external certifications and any notice of expiration	A.B. Data may only disclose certifications and expirations upon written request.
Crisis and Risk Management	Incident response / "disaster plan" for immediate response to security incidents such as data breach	A.B. Data has a formal written Incident Response Policy which addresses immediate security incidents. This plan addresses all levels of response and coordination which include management, security response teams, and law enforcement if required.
Crisis and Risk Management	Process and timing for notification to attorneys, claimants, and other stakeholders of a data breach and consideration of resources and/or remedies to provide thereto	A.B. Data has a formal written Incident Response Policy which addresses immediate security incidents. This plan addresses all levels of response and coordination which include management, security response teams, external partners, and law enforcement if required.
Crisis and Risk Management	Vendor management program that determines and defines requirements to manage risk associated with outsourcing	A.B. Data has a formal vendor management and risk management policy which defines requirements for vendors of A.B. Data. This policy is available for review upon request.
Physical Access Controls	Physical Access Security - Security Guards	A.B. Data contracts physical security monitoring to an accredited alarm monitoring company. As part of this contract, A.B. Data has access to security guards on patrol who will respond to issues at our facilities.
Physical Access Controls	Physical Access Security - Access cards to facilities with assignment of identification card subject to approval and review	A.B. Data utilizes access control cards (ACS) and identification cards to control physical access to its facilities. Cards are only issued through a management approval process.
Physical Access Controls	Physical Access Security - Logs of access	A.B. Data retains logs of all access to/from our facilities.
Physical Access Controls	Alarm Systems	AB Data utilizes multiple alarm systems which offer intrusion, fire, and duress alarms. These systems are monitored by certified third party monitoring companies and respond to alarms on a 24 hour basis, 7 days a week, 365 days per year.
Physical Access Controls	CCTV recording systems	AB Data manages CCTV and recording systems in house through its IT department management. Video recordings are maintained for 90 days for review retention. All building external entrances and exits are covered by CCTV recordings. In our datacenter, additional coverage is monitoring all exits and entrances along with coverage views of critical equipment and systems. All systems are maintained under a battery and generator power backup to ensure continuous coverage.
Data Collection and Retention	Minimization of collection of personally identifiable information, e.g., social security numbers and banking information	A.B. Data only requests information that is needed for purposes of settlement administration and approved by the Court. Typically complete social security numbers and banking information are not required.
Data Collection and Retention	Data collection only required to extent necessary for settlement administration	A.B. Data only requests information that is needed for purposes of settlement administration and approved by the Court. Typically complete social security numbers and banking information are not required.
Data Collection and Retention	Various methods for ensuring data protection and security - Data classification (including implementation of appropriate safeguards to protect from theft, loss, and/or unauthorized disclosure, use, access, destruction)	A.B. Data's Information Security Policy addresses all data classification and protection policies and procedures. Additionally A.B. Data's staff sign confidentiality and privacy agreements to ensure data is handled appropriately. These policies are available for review upon request.

Category	Control / Question	Response
Data Collection and Retention	Various methods for ensuring data protection and security - Compliance with applicable laws and regulations (see below)	A.B. Data's Information Security Policy addresses all data compliance and regulatory protections. These policies are available for review upon request.
Data Collection and Retention	Various methods for ensuring data protection and security - Secure Data Transfer	A.B. Data requires all data transfers to follow industry standard security requirements. A.B. Data's Information Security Policy details these requirements, which include use of encryption during data transfers along with additional security measures.
Data Destruction	Preservation of data only for so long as required for administration of the settlement and any relevant reporting required following the payments or distributions	A.B. Data retains settlement administration data based on the requirements set forth in relevant Court Order and/or client agreements. If no guidance is provided, A.B. Data destroys all data when no longer needed for purposes of settlement administration.
Data Destruction	Secure data destruction (e.g., 6 months – 1 year or when no longer required)	A.B. Data retains settlement administration data based on the requirements set forth in relevant Court orders and/or client agreements. If no guidance is provided, A.B. Data destroys all data when no longer needed for purposes of settlement administration.
Data Destruction	Physical media (e.g., paper, CDs) shredded or destroyed to point where they cannot be reconstructed	A.B. Data's Information Security Policy details physical media destruction requirements which meet industry standards. Electronic media that is being retired from service must be erased using the NIST Data Destruction Standard 800-88 Media Sanitation Procedures. If media is no longer functional, the media must be physically destroyed via shredding, degaussing, hammer, or other physical method to make the media fully unusable and severely difficult for physical reconstruction.
Data Destruction	Destruction of all derivative copies and/or back-ups	A.B. Data's Information Security Policy details physical media destruction requirements which meet industry standards. Electronic media that is being retired from service must be erased using the NIST Data Destruction Standard 800-88 Media Sanitation Procedures. If media is no longer functional, the media must be physically destroyed via shredding, degaussing, hammer, or other physical method to make the media fully unusable and severely difficult for physical reconstruction.
Applicable Laws, Standards, and Other Regulation	Industry standards: National Institute of Standards and Technology (NIST), HIPAA, FISMA, System and Organization Controls (SOC1 and SOC2) or more advanced assessment, ISO 27001	A.B. Data follows all applicable local, national, and international privacy regulations. A.B. Data's security team facilitates and monitors compliance with privacy policies.
Applicable Laws, Standards, and Other Regulation	Local, national, international privacy regulations (including CCPA)	A.B. Data follows all applicable local, national, and international privacy regulations. A.B. Data's security team facilitates and monitors compliance with privacy policies.
Ethical Rules	Administrative policies and/or employee handbook incorporating commitment to ethical rules (e.g., company, court ethical rules) setting forth standards of ethical and legal behavior	All employees are subject to the terms of A.B. Data's Employee Handbook which outlines all employee administrative policies, obligations, and requirements.
Ethical Rules	Enforcement clauses, violation resulting in disciplinary action including and up to termination of employment	Consequences of employee breaches of administrative policies is subject to management discretion.
Customer Service Measures	Description of settlement website and posting thereto of relevant privacy policies or statements (including portal for reporting suspected loss of confidential data submitted with claim)	All settlement websites contain a link to A.B. Data's privacy policy and, for dynamic websites where A.B. Data collects data, A.B. Data utilize an SSL certificate that authenticates a website's identity and enables an encrypted connection.

Category	Control / Question	Response
Customer Service Measures	Explanation of role of claims administrator and how to prevent phishing (e.g., clear indication that administrator will not request confidential information by e-mail and how to identify a valid email sent from the administrator)	<p>Emails sent to class members are written in concise language, contain prominent links to the settlement website, and include an explanation of how the email is related to a court-approved settlement. A.B. Data never requests that confidential information be sent over email. A.B. Data also implements certain best practices when disseminating email to minimize confusion and maximize deliverability. For example, the subject line, the sender, and the body of the message will be designed to overcome SPAM filters and encourage readership. Emails are sent in an embedded html text format without graphics, tables, images, attachments, and other elements that would increase the likelihood that the message could be blocked by an e-mail service provider or labeled as SPAM. Emails are also transmitted with a digital signature to the header and content, which allows e-mail service providers to programmatically authenticate that the emails are from A.B. Data's authorized mail servers.</p>

EXHIBIT B

1 **KESSLER TOPAZ MELTZER**
 2 **& CHECK, LLP**
 3 JENNIFER L. JOOST (Bar No. 296164)
 4 (jjoost@ktmc.com)
 5 STACEY M. KAPLAN (Bar No. 241989)
 6 (skaplan@ktmc.com)
 7 One Sansome Street, Suite 1850
 8 San Francisco, CA 94104
 9 Tel: (415) 400-3000
 10 Fax: (415) 400-3001

11 *Counsel for Class Representative SEB Investment*
 12 *Management AB and Class Counsel*

13 **UNITED STATES DISTRICT COURT**
 14 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
 15 **SAN FRANCISCO DIVISION**

16 SEB INVESTMENT MANAGEMENT AB, and
 17 WEST PALM BEACH FIREFIGHTERS’
 18 PENSION FUND, Individually and on Behalf of
 19 All Others Similarly Situated,

20 Plaintiffs,

21 v.

22 WELLS FARGO & COMPANY, CHARLES W.
 23 SCHARF, KLEBER R. SANTOS, and CARLY
 24 SANCHEZ,

25 Defendants.

Case No. 22-cv-03811-TLT

**DECLARATION OF SHARAN
 NIRMUL IN RESPONSE TO
 THE COURT’S SUPPLEMENTAL
 QUESTIONS FOR THE HEARING**

1 Sharan Nirmul declares as follows:

2 1. I, Sharan Nirmul, am a partner in the law firm Kessler Topaz Meltzer & Check, LLP
3 (“Kessler Topaz” or “Class Counsel”), counsel of record for Class Representatives SEB Investment
4 Management AB and West Palm Beach Firefighters’ Pension Fund and the Court-certified Class in
5 the above-captioned action (“Action”).

6 2. I, on behalf of Class Counsel, respectfully submit the following responses to the
7 Court’s Supplemental Questions for the Hearing (Dkt. No. 276). Specifically, I provide information
8 regarding Class Counsel’s selection of A.B. Data, Ltd. as the Claims Administrator for the
9 Settlement and its conclusion that A.B. Data’s retention was and continues to be in the best interests
10 of the Class. I also provide information regarding the due diligence Class Counsel has performed
11 and/or will perform regarding A.B. Data’s approach to: (i) financial disclosures and revenue sharing;
12 (ii) fees and residuals; (iii) data privacy; (iv) use of artificial intelligence; and (v) fraud prevention.

13 **I. A.B. Data’s Selection as Administrator**

14 3. A.B. Data was initially proposed and retained as the administrator in connection with
15 providing notice of the pendency of the Action as a class action (“Class Notice”) in July 2025. Dkt.
16 No. 230. Prior to A.B. Data’s retention, Class Counsel performed a formal bidding process,
17 soliciting proposals for notice and administration services from five experienced settlement
18 administration firms, including A.B. Data. Class Counsel requested that each of the firms describe
19 their qualifications and set forth their proposed fees and costs for Class Notice as well as their
20 proposed fees and costs for settlement notice and administration. *See* Declaration of Sharan Nirmul
21 in Support of Plaintiffs’ Unopposed Motion for Preliminary Approval of Settlement (Dkt. No. 254-
22 2), at ¶¶ 4-5. During this process, Class Counsel carefully reviewed the bids received and reached
23 out to certain of the administrators with follow-up questions. A.B. Data’s proposed fees and cost
24 structures resulted in the lowest estimated total cost of the five bids received. In addition to its
25 competitive pricing—and ultimate cost savings for the Class, Class Counsel believed that A.B. Data
26 possessed the requisite experience and capacity to reliably and competently administer Class Notice
27 (as well as to notice and administer a potential settlement of the Action). *Id.* at ¶ 5. Class Counsel

1 believes that A.B. Data has been and continues to be a reliable and competent administrator and
2 continues to serve the best interests of the Class in the Action.

3 4. In proposing (and ultimately retaining) A.B. Data as the Administrator for Class
4 Notice and later, as the Claims Administrator for the Settlement, there was no potential conflict of
5 interest or potential appearance of conflict of interest in Class Counsel’s selection of A.B. Data. As
6 noted above, A.B. Data’s selection was the result of a competitive bidding process between five
7 potential administrators. Moreover, there is no past or current financial relationship between Class
8 Counsel and A.B. Data.

9 **II. Class Counsel's Due Diligence**

10 **A. Financial Disclosures and Revenue Sharing**

11 5. At the outset of their engagement, Class Counsel confirmed that A.B. Data would
12 not be receiving any revenue or financial benefit beyond the fees and costs set forth in their pricing
13 proposal. A.B. Data included this confirmation in the Declaration of Eric A. Nordskog in Support
14 of Plaintiffs’ Unopposed Motion for Preliminary Approval of Settlement (Dkt. No. 254-3, at ¶ 7)
15 (“Notice Plan Decl.”) (“A.B. Data will not receive any additional revenue beyond what is detailed
16 in its proposal. A.B. Data also confirms that it does not have any financial arrangements with any
17 third parties that are related to the administration of the Settlement.”).

18 **B. Fees and Residuals**

19 6. As requested by Class Counsel, all fees and charges expected to be incurred by A.B.
20 Data in connection with the administration of the Settlement were set forth in A.B. Data’s pricing
21 proposal provided to Class Counsel during the formal bidding process described in Paragraph 3
22 above. Class Counsel carefully reviewed A.B. Data’s proposal for the scope of those fees and
23 charges. Prior to incurring any “out of scope” fees or charges not included in its proposal, A.B. Data
24 will notify and seek Class Counsel’s approval for these fees/charges.

25 7. There will be no interchange fees, dormancy fees, or retention of residual balances
26 in connection with the administration of the Settlement as these fees apply in cases where, unlike
27

1 here, class member payments are made by pre-paid credit card. Here, payments to Class Members
2 will be made either by check or wire transfer.

3 **C. Data Privacy**

4 8. In accordance with the Northern District of California's *Procedural Guidance for*
5 *Class Action Settlements*, A.B. Data's data privacy controls and procedures (including technical,
6 administrative, and physical controls; retention; destruction; audits; and crisis response; etc.) were
7 detailed in a Chart attached as Exhibit B to the previously-filed Notice Plan Declaration. *See* Dkt.
8 No. 254-3, at ¶¶ 3-5 & Ex. B. Class Counsel carefully reviewed this Chart and conferred with A.B.
9 Data regarding the provisions.

10 **D. Use of Artificial Intelligence**

11 9. A.B. Data's pricing proposal and scope of work provided to Class Counsel during
12 the formal bidding process described in Paragraph 3 above did not include the utilization of artificial
13 intelligence for any of its work administering the Settlement, and it is Class Counsel's understanding
14 that A.B. Data is not using artificial intelligence to administer the Settlement. In the event A.B. Data
15 determines that the use of artificial intelligence would be useful in some aspect of this
16 administration, A.B. Data will confer with Class Counsel before using artificial intelligence.

17 **E. Fraud Prevention**

18 10. Class Counsel is familiar with the fraud prevention measures A.B. Data utilizes in
19 its administrations from its prior experience working with A.B. Data. In administering the
20 Settlement, A.B. Data will report potentially fraudulent Claims to Class Counsel in real-time in
21 certain circumstances. For example, if A.B. Data discovers a potentially fraudulent Claim with large
22 losses or which could be linked to a broader fraudulent claim filing pattern, A.B. Data will notify
23 Class Counsel right away and Class Counsel and A.B. Data will confer on next steps. Barring those
24 unique circumstances, A.B. Data will provide Class Counsel with a report of all potentially
25 fraudulent claims at the conclusion of the administration.

1 I declare under penalty of perjury that the foregoing is true and correct.

2 Executed on this 30th day of April 2026, in Radnor, Pennsylvania.

3
4 

5

Sharan Nirmul

6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28