or bank holding company. The factors that are considered in acting on the applications are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The public portions of the applications listed below, as well as other related filings required by the Board, if any, are available for immediate inspection at the Federal Reserve Bank(s) indicated below and at the offices of the Board of Governors. This information may also be obtained on an expedited basis, upon request, by contacting the appropriate Federal Reserve Bank and from the Board's Freedom of Information Office at *https://www.federalreserve.gov/foia/request.htm.* Interested persons may express their views in writing on the standards enumerated in paragraph 7 of the Act.

Comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors, Ann E. Misback, Secretary of the Board, 20th Street and Constitution Avenue, NW, Washington DC 20551–0001, not later than February 27, 2024.

A. Federal Reserve Bank of St. Louis (Holly A. Rieser, Senior Manager) P.O. Box 442, St. Louis, Missouri 63166–2034. Comments can also be sent electronically to *Comments.applications@stls.frb.org:*

1. *Bennie F. Ryburn, III, Ray Morrison Ryburn, Marion B. Ryburn, and Halley A. Ryburn, all of Monticello, Arkansas; Angelia D. Ryburn, Wilmar, Arkansas; Margaret Anne Ryburn, Atlanta, Georgia; and Madison A. Ryburn, Dallas, Texas;* to join the Ryburn Family Control Group, a group acting in concert, to retain voting shares of Drew Bancshares, Inc., and thereby indirectly retain voting shares of Commercial Bank & Trust Company, both of Monticello, Arkansas.

2. *The Michael F. Bender Revocable Living Trust dated February 10, 2023, and The Diane M. Bender Revocable Living Trust dated February 10, 2023, Michael F. Bender and Diane M. Bender as co-trustees of both trusts, all of Farmington, Missouri;* to retain voting shares of Midwest Regional Bancorp, Inc., Festus, Missouri, and thereby indirectly retain voting shares of Midwest Regional Bank, Clayton, Missouri.

A. Federal Reserve Bank of Kansas City (Jeffrey Imgarten, Assistant Vice President) 1 Memorial Drive, Kansas City, Missouri, 64198–0001. Comments can also be sent electronically to *KCApplicationComments@kc.frb.org:*

1. *Daniel J. Murphy, Elkhorn, Nebraska;* to join the Murphy Family Control Group, a group acting in concert, to acquire voting shares of Ameriwest Corporation, and thereby indirectly acquire voting shares of First Westroads Bank, Inc., both of Omaha, Nebraska.

Board of Governors of the Federal Reserve System.

Michele Taylor Fennell,

Deputy Associate Secretary of the Board.

[FR Doc. 2024–02848 Filed 2–12–24; 8:45 am]

BILLING CODE P

FEDERAL RESERVE SYSTEM

Change in Bank Control Notices; Acquisitions of Shares of a Bank or Bank Holding Company

The notificants listed below have applied under the Change in Bank Control Act (Act) (12 U.S.C. 1817(j)) and 225.41 of the Board's Regulation Y (12 CFR 225.41) to acquire shares of a bank or bank holding company. The factors that are considered in acting on the applications are set forth in paragraph 7 of the Act (12 U.S.C. 1817(j)(7)).

The public portions of the applications listed below, as well as other related filings required by the Board, if any, are available for immediate inspection at the Federal Reserve Bank(s) indicated below and at the offices of the Board of Governors. This information may also be obtained on an expedited basis, upon request, by contacting the appropriate Federal Reserve Bank and from the Board's Freedom of Information Office at *https://www.federalreserve.gov/foia/request.htm.* Interested persons may express their views in writing on the standards enumerated in paragraph 7 of the Act.

Comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors, Ann E. Misback, Secretary of the Board, 20th Street and Constitution Avenue NW, Washington, DC 20551–0001, not later than February 28, 2024.

A. Federal Reserve Bank of St. Louis (Holly A. Rieser, Senior Manager) P.O. Box 442, St. Louis, Missouri 63166–2034. Comments can also be sent electronically to *Comments.applications@stls.frb.org:*

1. *Rondal L. Wright Irrevocable Grantor Trust, R. Brent Wright, individually and as trustee, both of Glasgow, Kentucky;* to acquire voting shares of Buffalo Bancshares, Inc., and thereby indirectly acquire voting shares of Bank of Buffalo, both of Buffalo, Kentucky.

Board of Governors of the Federal Reserve System.

Michele Taylor Fennell,

Deputy Associate Secretary of the Board.

[FR Doc. 2024–02947 Filed 2–12–24; 8:45 am]

BILLING CODE P

FEDERAL TRADE COMMISSION

[File No. 202 3181]

Blackbaud, Inc.; Analysis of Proposed Consent Order To Aid Public Comment

AGENCY: Federal Trade Commission.

ACTION: Proposed consent agreement; request for comment.

SUMMARY: The consent agreement in this matter settles alleged violations of federal law prohibiting unfair or deceptive acts or practices. The attached Analysis of Proposed Consent Order to Aid Public Comment describes both the allegations in the complaint and the terms of the consent order—embodied in the consent agreement—that would settle these allegations.

DATES: Comments must be received on or before March 14, 2024.

ADDRESSES: Interested parties may file comments online or on paper by following the instructions in the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Please write ''Blackbaud, Inc.; File No. 202 3181'' on your comment and file your comment online at *https://www.regulations.gov* by following the instructions on the web-based form. If you prefer to file your comment on paper, please mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Mail Drop H–144 (Annex D), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT: Cathlin Tully (202–326–3644), Attorney, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: Pursuant to section 6(f) of the Federal Trade Commission Act, 15 U.S.C. 46(f), and FTC Rule 2.34, 16 CFR 2.34, notice is hereby given that the above-captioned consent agreement containing a consent order to cease and desist, having been filed with and accepted, subject to final approval, by the Commission, has been placed on the public record for a period of 30 days. The following Analysis to Aid Public Comment describes the terms of the consent agreement and the allegations in the complaint. An

electronic copy of the full text of the consent agreement package can be obtained at *https://www.ftc.gov/news-events/commission-actions.*

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before March 14, 2024. Write ''Blackbaud, Inc.; File No. 202 3181,'' on your comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including, to the extent practicable, on the *https://www.regulations.gov* website.

Because of heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comments online through the *https://www.regulations.gov* website. If you prefer to file your comment on paper, write ''Blackbaud, Inc.; File No. 202 3181'' on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Mail Drop H–144 (Annex D), Washington, DC 20580.

Because your comment will be placed on the publicly accessible website at *https://www.regulations.gov,* you are solely responsible for making sure your comment does not include any sensitive or confidential information. In particular, your comment should not include sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure your comment does not include sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any ''trade secret or any commercial or financial information which . . . is privileged or confidential''—as provided by Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2)—including competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled ''Confidential,'' and must comply with FTC Rule § 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request and must identify the specific portions of the comment to be withheld from the public record. *See* FTC Rule § 4.9(c). Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted on the *https://www.regulations.gov* website—as legally required by FTC Rule § 4.9(b)—we cannot redact or remove your comment from that website, unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule § 4.9(c), and the General Counsel grants that request.

Visit the FTC website at *https://www.ftc.gov* to read this document and the news release describing the proposed settlement. The FTC Act and other laws the Commission administers permit the collection of public comments to consider and use in this proceeding, as appropriate. The Commission will consider all timely and responsive public comments it receives on or before March 14, 2024. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see *https://www.ftc.gov/site-information/privacy-policy.*

Analysis of Proposed Consent Order To Aid Public Comment

The Federal Trade Commission (the ''Commission'') has accepted, subject to final approval, an agreement containing consent order from Blackbaud, Inc. (''Respondent'' or ''Blackbaud''). The proposed consent order (''Proposed Order'') has been placed on the public record for 30 days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After 30 days, the Commission will again review the agreement, along with any comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the Proposed Order.

Blackbaud is a publicly traded South Carolina corporation that provides a variety of data services and financial, fundraising, and administrative software solutions to over 45,000 companies, nonprofits, foundations, educational institutions, healthcare organizations, and individual customers throughout the U.S. and abroad. Blackbaud maintains the personal information of millions of U.S. consumers that have donor, student, patient, and other relationships with Blackbaud's customers.

According to the FTC's Complaint, despite representing that it would protect consumers' data from unauthorized access through a variety of safeguards, from February through May 2020, Blackbaud's networks suffered a data breach from an attacker that exfiltrated data from thousands of Blackbaud customers. This data comprised millions of consumers' personal information, including, in some cases, sensitive information including social security numbers and financial information. Adding to the scope and severity of the breach was Blackbaud's indefinite retention of customer backup files, which impacted additional current, prospective, and former customers, whose consumer data would not have otherwise been impacted by the data breach. And when Blackbaud informed customers of the breach in July 2020, its initial breach notification statement inaccurately stated that the hacker had not stolen sensitive consumer data. Blackbaud did not correct this information until October 2020, despite knowing it was inaccurate only a couple of weeks after the initial breach notification.

The Commission's proposed five-count complaint alleges that Respondent violated section 5(a) of the FTC Act by (1) failing to employ reasonable information security practices to protect consumers' personal information; (2) failing to implement and enforce reasonable data retention practices; (3) failing to accurately communicate about the breach in its initial breach notification; (4) misrepresenting that it used appropriate safeguards to protect consumers' personal information; and (5) misrepresenting the scope of the breach by stating that consumers' personal information had not been impacted by the breach in its initial notification. With respect to the first count, the proposed complaint alleges that Respondent:

- failed to implement appropriate password controls, which resulted in employees often using default, weak or identical passwords;
- failed to apply adequate multifactor authentication for both employees and customers to protect sensitive consumer information;
- failed to prevent data theft by (1) monitoring for unauthorized attempts to transfer or exfiltrate consumers' personal information from its networks; (2) continuously logging and monitoring its systems and assets to identify data security events; and (3) performing regular assessments as to the effectiveness of protection measures;

• failed to implement and enforce appropriate data retention schedules and deletion practices for the vast amounts of consumers' personal information stored on its network;

• failed to patch outdated software and systems in a timely manner;

• failed to test, audit, assess or review its products' or applications' security features; and conduct regular risk assessments, vulnerability scans, and penetration testing of its networks and databases;

• failed to implement appropriate firewall controls; and

• failed to implement appropriate network segmentation to prevent attackers from moving freely across its networks and databases.

The proposed complaint alleges that Respondent could have addressed each of these failures by implementing readily available and relatively low-cost security measures. With respect to the second count, the proposed complaint alleges that Respondent failed to implement and enforce reasonable data retention practices for sensitive consumer data maintained by its customers on its network. With respect to the third count, the proposed complaint alleges that Respondent failed to accurately communicate the scope and severity of the breach in its initial notification to consumers.

The proposed complaint alleges that, with respect to counts one, two, and three, Respondent's failures caused, or are likely to cause, substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. Such practices constitute unfair acts or practices under section 5 of the FTC Act.

With respect the fourth count, the proposed complaint alleges that, at various times, Respondent claimed that is used appropriate safeguards to protect consumers' personal information. The proposed complaint alleges that, in reality, and as noted above, Respondent failed to implement reasonable measures to protect consumer's personal information. Such representations were deceptive under section 5 of the FTC Act.

With respect to the fifth count, the proposed complaint alleges that, in its initial breach notification, Respondent claimed that consumers' personal information had not been subject to the breach. The proposed complaint alleges that, in reality, and as noted above, consumers' personal information had been exfiltrated by the attacker in the breach. Such representations were, therefore, deceptive under section 5 of the FTC Act.

Summary of the Proposed Order With Respondent

The Proposed Order contains injunctive relief designed to prevent Respondent from engaging in the same or similar acts or practices in the future. Part I prohibits Respondent from misrepresenting the extent (1) to which it maintains, uses, deletes or disclosed consumers' personal information; (2) to which it protects the privacy, security, availability, confidentiality, or integrity of consumers' personal information; or (3) of any future data security incident or unauthorized disclosure of consumers' personal information.

Part II requires Respondent to delete or destroy customer backup files containing consumers' personal information that are not being retained to provide its products or services and to refrain from maintaining consumers' personal information that is not necessary for the purposes for which it is maintained by Respondent. Part III requires that Respondent document and adhere to a retention schedule for its customer backup files containing consumers' personal information, including the purposes for which it maintains such information, the business needs for its retention, and the timeframe for its deletion.

Part IV requires that Respondent establish and implement, and thereafter maintain, a comprehensive information security program that protects the security, availability, confidentiality, and integrity of consumers' personal information. Part V requires Respondent to obtain initial and biennial information security assessments by an independent, third-party professional for 20 years. Part VI requires Respondent to disclose all material facts to the assessor required by Part V and prohibits Respondent from misrepresenting any fact material to the assessments required by Part IV.

Part VII requires Respondent to submit an annual certification from its Chief Information Security Officer that the company has implemented the requirements of the Order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission. Part VIII requires Respondent to notify the Commission any time it notifies a federal, state, or local government that consumer personal information was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.

Parts IX–XII are reporting and compliance provisions, which include recordkeeping requirements and provisions requiring Respondent to provide information or documents necessary for the Commission to monitor compliance. Part XIII states that the Proposed Order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to facilitate public comment on the Proposed Order, and it is not intended to constitute an official interpretation of the complaint or Proposed Order, or to modify the Proposed Order's terms in any way.

By direction of the Commission.

April J. Tabor,

Secretary.

Joint Statement of Chair Lina M. Khan, Commissioner Rebecca Kelly Slaughter, and Commissioner Alvaro M. Bedoya

Today the FTC brings an enforcement action against Blackbaud for a series of unfair and deceptive data security practices. Blackbaud provides backend services for a variety of entities, ranging from businesses and nonprofits to schools and healthcare organizations. As noted in the FTC's complaint, Blackbaud in 2020 was struck by a data breach that exposed the personal data of millions of Americans. The FTC charges that Blackbaud's reckless data retention practices rendered its security failures much more costly: by hoarding reams of data that it did not reasonably need, Blackbaud's breach exposed far more data. Moreover, Blackbaud's notification alerting victims of the breach included false statements, which Blackbaud did not correct until months later—and months after it knew the statements were false.

The FTC's complaint alleges that Blackbaud's practices violated Section 5's prohibition on unfair or deceptive practices. The complaint marks a new step forward by alleging standalone unfairness counts for (a) failure to implement and enforce reasonable data retention practices (Count II) and (b) failure to accurately communicate the scope and severity of the breach in its notification to consumers (Count III).[1] Blackbaud's data retention failures exacerbated the harms of its data security failures because Blackbaud had failed to delete data it no longer needed. This action illustrates how indefinite retention of consumer data, which can lure hackers and magnify the harms stemming from a breach, is independently a prohibited unfair practice under the FTC Act. Similarly, Blackbaud's failure to accurately convey

[1] Complaint, *In re Blackbaud, Inc.,* Docket No. C–4804 (Jan. 30, 2024) ¶¶ 29–34, *https://www.ftc.gov/system/files/ftc_gov/pdf/Blackbaud-Complaint.pdf.*

the scope and severity of the breach kept victims in the dark and delayed them from taking protective actions, making a bad situation even worse.

Today's action builds on a series of cases that have made clear that maintaining a data retention and deletion schedule is a critical part of protecting consumers' data security.[2] The Commission has also made clear that efforts to downplay the extent or severity of a data breach run afoul of the law.[3]

We are grateful to the Division of Privacy and Identity Protection for their excellent work, which enables us to continue making key strides in protecting people's data. As businesses face fresh incentives to hoard data to train AI models,[4] protecting Americans from unlawful data practices will be especially critical.

[FR Doc. 2024–02970 Filed 2–12–24; 8:45 am]

BILLING CODE 6750–01–P

[2] *See, e.g.,* Press Release, Fed. Trade Comm'n, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards (Dec. 19, 2023), *https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without;* Press Release, Fed. Trade Comm'n, FTC Finalizes Order With Online Alcohol Marketplace For Security Failures That Exposed Personal Data of 2.5 Million People (Jan. 10, 2023), *https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-finalizes-order-online-alcohol-marketplace-security-failures-exposed-personal-data-25-million;* Press Release, Fed. Trade Comm'n, FTC Brings Action Against Ed Tech Provider Chegg for Careless Security that Exposed Personal Data of Millions of Customers (Oct. 31, 2022); Press Release, Fed. Trade Comm'n, FTC Takes Action Against Global Tel*Link Corp. for Failing to Adequately Secure Data, Notify Consumers After Their Personal Data Was Breached (Nov. 16, 2023), *https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-takes-action-against-global-tellink-corp-failing-adequately-secure-data-notify-consumers-after. See also* FTC Technology Blog, Security Principles: Addressing Underlying Causes of Risk in Complex Systems (Feb. 1, 2023), *https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems.*

[3] *See, e.g.,* Press Release, Fed. Trade Comm'n, FTC Takes Action Against CafePress for Data Breach Cover Up (Mar. 15, 2022), *https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover. See also* FTC Technology Blog, Security Beyond Prevention: The Importance of Effective Breach Disclosures (May 20, 2022), *https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2022/05/security-beyond-prevention-importance-effective-breach-disclosures.*

[4] Press Release, Fed. Trade Comm'n, FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Request (May 31, 2023), *https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever.*

GENERAL SERVICES ADMINISTRATION

[Notice-PBS–2024–02; Docket No. 2024–0002; Sequence No.3]

Notice of Availability of a Draft Environmental Impact Statement for the Alcan Land Port of Entry Expansion and Modernization in Alcan, Alaska; Withdrawal

AGENCY: Public Buildings Service, General Services Administration (GSA).

ACTION: Notice; withdrawal.

SUMMARY: GSA is announcing the withdrawal of the Notice of availability of a draft environmental impact statement for the Alcan land port of entry expansion and modernization in Alcan, Alaska. The February 7,2024 notice announced GSAs intent to prepare a Draft Environmental Impact Statement (DEIS) to analyze the potential environmental effects of the proposed expansion and modernization of the existing Alcan LPOE.

FOR FURTHER INFORMATION CONTACT: Aaron Evanson, Capital Project Manager, (206) 445–5876, *AlcanLPOE@gsa.gov.*

SUPPLEMENTARY INFORMATION: The Notice of availability published in the **Federal Register** on February 7, 2024. GSA plans to publish at a later date.

Lois Mandell,

Director Regulatory Secretariat Division, Office of Government-wide Policy.

[FR Doc. 2024–02847 Filed 2–12–24; 8:45 am]

BILLING CODE 6820–DL–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Notice of Closed Meeting

Pursuant to 5 U.S.C. 1009(d), notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended, and the Determination of the Director, Office of Strategic Business Initiatives, Office of the Chief Operating Officer, CDC, pursuant to Public Law 92–463. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: Disease, Disability, and Injury Prevention and Control Special Emphasis Panel (SEP)—SIP24–012, Advancing Research in Immunization Services Network (ARISe Network).

Date: May 14, 2024.

Time: 10 a.m.–6 p.m., EDT.

Place: Teleconference/Web Conference.

Agenda: To review and evaluate grant applications.

For Further Information Contact: Catherine Barrett, Ph.D., Scientific Review Officer, National Center for Chronic Disease Prevention and Health Promotion, Centers for Disease Control and Prevention, 4770 Buford Highway, Mailstop S106–3, Atlanta, Georgia 30341–3717. Telephone: (404) 718–7664; Email: *CBarrett@cdc.gov.*

The Director, Office of Strategic Business Initiatives, Office of the Chief Operating Officer, Centers for Disease Control and Prevention, has been delegated the authority to sign **Federal Register** notices pertaining to announcements of meetings and other committee management activities, for both the Centers for Disease Control and Prevention and the Agency for Toxic Substances and Disease Registry.

Kalwant Smagh,

Director, Office of Strategic Business Initiatives, Office of the Chief Operating Officer, Centers for Disease Control and Prevention.

[FR Doc. 2024–02885 Filed 2–12–24; 8:45 am]

BILLING CODE 4163–18–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

Notice of Closed Meeting

Pursuant to 5 U.S.C. 1009(d), notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), title 5 U.S.C., as amended, and the Determination of the Director, Office of Strategic Business Initiatives, Office of the Chief Operating Officer, CDC, pursuant to Public Law 92–463. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.