Orange Bank & Trust Company Notifies Individuals of The Mercadien Group Data Security Incident

Orange Bank & Trust Company ("OB&T") is committed to maintaining the privacy and security of personal information. OB&T recently notified individuals of a data security incident involving its accounting and advisory services vendor, Mercadien, P.C. CPAs ("Mercadien"). Mercadien recently discovered a data security incident that may have affected OB&T's and related institution customer information.

The incident involved Box.com data, a third-party data hosting platform utilized by Mercadien to support services it provides to OB&T and its related institutions. Box.com is a commonly used secure Managed File Transfer ("MFT") software supporting file transfer activities by thousands of organizations around the world. Mercadien promptly launched an investigation into the nature and scope of the impact on its systems and discovered that the unauthorized activity in the Box.com environment occurred between September 17, 2025, and October 8, 2025. During that time, unauthorized actors obtained OB&T vendor files transferred via Box.com.

Importantly, the incident did not involve any of OB&T's systems and did not impact OB&T's ability to serve its customers.

Upon learning of the incident, OB&T immediately began efforts to remediate the issue and commenced a prompt and thorough investigation. As part of its investigation, OB&T worked very closely with external cybersecurity professionals experienced in handling these types of incidents. Following the completion of the investigation, OB&T discovered on August 28, 2026, that a limited number of files which were potentially subject to unauthorized access or acquisition between September 17, 2025, and October 8, 2025, contained personal information. The following information may have been impacted: name, financial and/or bank account information, passport number, dates of birth, government identification number, taxpayer identification number, and Social Security number. Not all information was impacted for all individuals.

OB&T has no evidence that any data has been misused. However, out of an abundance of caution, on September 2, 2026, OB&T is sending notification letters in accordance with state and federal law to each potentially affected individual for whom they have a last known address. OB&T is providing notified individuals with best practices to protect their information and offering complimentary credit monitoring services for those who had their Social Security number impacted. OB&T encourages impacted individuals to take actions to help protect their personal information. These actions include placing a fraud alert and/or security freeze on their credit files, and/or obtaining a free credit report. Additionally, individuals should always remain vigilant in reviewing their financial account statements, explanation of benefits statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities.

OB&T remains fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it, including continually evaluating and modifying its practices and internal controls. Please be assured that OB&T, along with Mercadien, are taking steps to address the incident and to help protect the security of your data.

For further questions about this incident, or to determine if you are affected, you may contact the dedicated response line at 833-931-3792 (code B171707), available Monday through Friday from 8 am – 8 pm Central time, excluding holidays.

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert.**

We recommend that you place a one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	Experian	TransUnion
P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (888) 378-4329	P.O. Box 9554 Allen, TX 75013 www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016 www.transunion.com/fraud-alerts (800) 680-7289

2. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348-5788 www.equifax.com/personal/credit-report-services/credit-freeze/ (888) 298-0045	P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze/center.html (888) 397-3742	P.O. Box 160 Woodlyn, PA 19094 www.transunion.com/credit-freeze (888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. If you do place a security freeze prior to enrolling in a credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.