BELLENFANT
CERTIFIED PUBLIC ACCOUNTANTS

# Notice of Data Event

Bellenfant PLLC (hereinafter "Bellenfant") is providing this substitute notice as a result of a security incident to provide individuals with information about the incident and to share resources available for those who wish to further safeguard their personal information.

Bellenfant discovered it was the victim of an unknown third party gaining unauthorized access to the Bellenfant network environment. Bellenfant discovered the incident on approximately July 23, 2025.

Upon learning of the issue, Bellenfant immediately engaged the appropriate forensic consultants to investigate the root of the incident, secure its systems, prevent this issue from reoccurring, and identify any sensitive or personal information that may have been impacted as a result.

Our investigation determined that data may have been exposed without authorization. Thereafter, Bellenfant conducted a thorough review of the contents of the files to determine if they contained any sensitive information. On October 2, 2025, after completing the extensive and exhaustive review, Bellenfant learned certain personal or sensitive information contained in its environment may have been exposed as result of the incident. Since that time, Bellenfant has been working diligently and exhaustively to identify and obtain sufficient information in order to provide you with this notice. This review is now complete, and on October 22, 2025, Bellenfant mailed individual notices to those impacted by the incident, where it had a valid mailing address. The individualized letters explain what personal information may have been impacted because of this incident.

Nonetheless, this message constitutes a substitute notice for those individuals Bellenfant attempted to notify but was unable to reach whose names and certain sensitive information were impacted by the incident.

Individuals who would like to determine whether they were potentially impacted by this incident, please call 1-833-788-9712 Monday through Friday from 8 a.m. to 8 p.m. Eastern Time, excluding holidays.

Although Bellenfant is unaware of any actual or attempted misuse of any information, it is providing notice of this incident out of an abundance of caution and in compliance with applicable laws. It is also providing free credit monitoring, cyber monitoring, and identity theft protection services through IDX and Cyberscout to those impacted by this incident.

Privacy and security are our top priorities. We deeply regret that this incident occurred and will continue to implement the most stringent security protocols available to prevent incidents like this one in the future. For additional information and guidance, please review the Reference Guide below to help protect your personal information.

Those impacted by this incident can also enroll in the complimentary credit monitoring services for adults and complimentary cyber monitoring services for minors being offered by logging on to https://bfs.cyberscout.com/activate and following the provided instructions. When prompted, please provide the following adult offering code to receive the credit monitoring services.

The enrollment requires an internet connection and an email account. Please note that when signing up for monitoring services, individuals may be asked to verify personal information to ensure their protection and confirm their identity.

If you have questions or need assistance, please call at 1-833-788-9712 Monday through Friday from 8 a.m. to 8 p.m. Eastern Time, excluding holidays.

In addition to the complimentary services above, there are steps individuals can take to protect themselves:

- Individuals should be on the lookout and regularly monitor the explanation of benefits statements received from their health plan and statements from health care providers, as well as bank and credit card statements, credit reports, and tax returns, to check for any unfamiliar activity.

- If an individual believes they are the victim of a crime, they can contact local law enforcement authorities and file a police report.

- If individuals notice any health care services they did not receive listed on an explanation of benefits statement, they should contact their health plan or doctor.

- If individuals notice any suspicious activity on bank or credit card statements or on tax returns, they should immediately contact their financial institution and/or credit card company or relevant agency.

BELLENFANT
CERTIFIED PUBLIC ACCOUNTANTS

# REFERENCE GUIDE

**1. Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

**2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

**3. Telephone.** Contact IDX at 1-833-788-9712 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**4. Review your credit reports**. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

**Credit Bureaus**

| Equifax Fraud Reporting | Experian Fraud Reporting | TransUnion Fraud Reporting |
|---|---|---|
| 1-866-349-5191 | 1-888-397-3742 | 1-800-680-7289 |
| P.O. Box 105069 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348-5069 | Allen, TX 75013 | Chester, PA 19022-2000 |
| www.equifax.com | www.experian.com | www.transunion.com |

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.
**Please Note: No one is allowed to place a fraud alert on your credit report except you.**

**6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

**California Residents:** Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

**New Mexico Residents**: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**New York Residents:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

**North Carolina Residents:** Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.