**Centennial Bank**
**Happy State Bank**
(a division of Centennial Bank)

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

# NOTICE OF DATA BREACH

Dear <<Full Name>>:

We are committed to safeguarding the personal information of our customers. We are writing to inform you of an incident that may have resulted in the unauthorized disclosure of some of your personal information, including your Social Security number. We want to provide you with details about the incident, the steps we have taken in response, and the actions you can take to further protect your information.

***What Happened?*** Centennial Bank and Happy State Bank, a Division of Centennial Bank, ("Bank") use a third-party service provider, Fidelity Information Services ("FIS"), to assist with certain banking operations, including customer due diligence processes. On August 7, 2026, an FIS associate was preparing a secure email containing a Customer file for the Bank. The associate inadvertently sent the file to an unintended recipient—an employee at another regulated financial institution—who shared the same first name as the intended Bank contact.

On August 10, 2026, the unintended recipient opened the file, realized it did not pertain to their institution, closed it, and promptly notified FIS of the error. FIS reported this incident to the Bank on August 17, 2026.

***What Information Was Involved?*** The file that was inadvertently disclosed contained personal information, which may include:

- Full name
- Mailing address
- Date of birth
- Account information (including date opened, account number, balance, transaction type, and status)
- Customer and entity identification numbers
- Citizenship
- Tax information (including Federal Taxpayer ID for some individuals)
- Mailing preference
- Customer details (including occupation, status, and familial relations)
- Bank branch details

***What We Are Doing.*** Upon learning of this incident, FIS and the Bank took immediate steps to minimize any potential harm. FIS immediately recalled the email and terminated access to the file. The FIS associate immediately notified FIS's privacy incident response team, who initiated a formal investigation. FIS sent a formal request for deletion to the unintended recipient, who confirmed deletion of the file on August 14, 2026. The recipient financial institution issued a Certificate of Destruction on August 26, 2026, confirming and certifying that all copies of the file were destroyed, no copies or portions were retained, and the information was not used for any purpose, transferred to other systems or recipients, or included in electronic backups. The unintended recipient is an employee of a regulated financial institution and is bound by confidentiality obligations, including where such information is received erroneously. FIS has retrained the associate responsible and implemented enhanced validation procedures to prevent similar incidents in the future. The Bank conducted its own review of the incident to ensure all appropriate safeguards are in place. The Bank initiated enhanced monitoring of affected accounts. The Bank is coordinating with FIS to ensure appropriate remediation measures are implemented.

We have no indication that your information has been misused as a result of this incident, but we have arranged for you to receive a 24-month complimentary membership to identity monitoring services through Epiq – Credit Monitoring Solutions.

***What You Can Do.*** It is always advisable to remain vigilant for incidents of fraud or identity theft by regularly reviewing your account statements and free credit reports for any unauthorized activity. For additional guidance on identity theft prevention and Epiq Credit Monitoring Solutions, including instructions on how to activate your complimentary membership, please see the pages that follow this letter.

***For More Information.*** If you have any questions about this incident or would like additional assistance, please call our dedicated response line at 888-619-0944, available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. You may also write to us at: Centennial Bank, 620 Chestnut Street, Conway, AR 72032.

We sincerely regret any concern or inconvenience this incident may cause you. Protecting the security and privacy of your information remains a top priority for our Bank.

Sincerely,

Centennial Bank

<<Full Name>>
**Activation Code:** <<Activation Code>>
**Enrollment Deadline**: <<Enrollment Deadline>>
**Coverage Length:** 24 Months

## Epiq - Privacy Solutions ID
1B Credit Monitoring - Plus

**How To Enroll:**

1) Visit www.privacysolutionsid.com and click "Activate Account"
2) Enter the following activation code, **<<Activation Code>>** and complete the enrollment form
3) Complete the identity verification process
4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5) Enter your log-in credentials
6) You will be directed to your dashboard and activation is complete!

**Product Features:**

**1-Bureau Credit Monitoring with Alerts**
Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

**VantageScore® 3.0 Credit Score and Report[1]**
1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

**SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)**
Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

**Dark Web Monitoring**
Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

**Change of Address Monitoring**
Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

**Credit Protection**
3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

**Personal Info Protection**
Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

**Identity Restoration & Lost Wallet Assistance**
Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

**Up to $1M Identity Theft Insurance[2]**
Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

**Unauthorized Electronic Funds Transfer- UEFT[2]**
Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring - Plus, please call directly at **866.675.2006,** Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

1 The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore® credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

2 Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## ADDITIONAL STEPS YOU CAN TAKE

In addition to enrolling in the complimentary credit monitoring services described above, we recommend that you take the following precautionary steps to further protect yourself:

**Monitor Your Accounts.** We recommend that you remain vigilant over the next 12 to 24 months by regularly reviewing your account statements, credit reports, and Explanation of Benefits statements for any suspicious activity. If you notice any unauthorized transactions, contact your financial institution immediately.

**Review Your Credit Reports.** You are entitled to one free credit report per year from each of the three major credit reporting agencies. To obtain your free annual credit report, visit www.annualcreditreport.com or call 1-877-322-8228. You may also contact the credit reporting agencies directly:

- **Equifax:** PO Box 740241, Atlanta, GA 30374; www.equifax.com; 1-800-685-1111
- **Experian:** PO Box 2002, Allen, TX 75013; www.experian.com; 1-888-397-3742
- **TransUnion:** PO Box 2000, Chester, PA 19016; www.transunion.com; 1-800-916-8800

**Place a Fraud Alert.** You may place a free fraud alert on your credit file by contacting any one of the three credit reporting agencies listed above. A fraud alert tells creditors to take extra steps to verify your identity before opening a new account in your name. An initial fraud alert lasts one year and can be renewed. Once you place a fraud alert with one agency, that agency will notify the other two.

**Place a Security Freeze.** You have the right to place a security freeze on your credit report free of charge. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your written authorization. Placing a security freeze may delay or interfere with the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. To place a security freeze, contact each of the three credit reporting agencies listed above.

**Report Suspicious Activity.** If you believe you are the victim of identity theft or fraud, you should contact your local law enforcement agency and file a report. You may also file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or by calling 1-877-438-4338, or by writing to: Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

**Massachusetts Residents:** Under Massachusetts law, you have the right to file and obtain a copy of a police report relating to this incident. You also have the right to request a security freeze on your credit report at no charge. You may contact the Massachusetts Office of the Attorney General at: One Ashburton Place, Boston, MA 02108; 1-617-727-8400; www.mass.gov/ago.