

## APPENDIX

CNB contracts with Fiserv for payment and financial services technology. Fiserv uses MOVEit Transfer by Progress Software, which is a commonly used secure Managed File Transfer software supporting file transfer activities by thousands of organizations around the world. On August 3, 2023, CNB learned that there was unauthorized access to Fiserv's MOVEit Transfer environment between May 27, 2023 and May 31, 2023, and during that period of time, unauthorized actors obtained files transferred via MOVEit Transfer. None of CNB's systems were involved in this incident.

After gathering the information needed to notify the involved individuals, Fiserv reported that additional files associated with CNB were involved. In an effort to minimize consumer confusion by consolidating the notification populations, CNB worked with Fiserv to combine the data and collect the information needed to notify the additional individuals. That process was completed on October 26, 2023. It was determined that one or more of the files in Fiserv's MOVEit Transfer environment contained the personal information of four Maine residents including their names and financial account numbers.

On November 15, 2023, Fiserv will mail notification letters on CNB's behalf via United States Postal Service First-Class mail to the individuals whose information was involved, including the Maine residents.<sup>1</sup> A sample of the notification letter is enclosed. The Maine residents are being offered a two-year, complimentary membership in credit monitoring and identity theft protection services through Kroll. A dedicated call center has been established for individuals to call with questions about the incident.

To help prevent something like this happening again, Fiserv has remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. Fiserv also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities.

---

<sup>1</sup> This report does not waive CNB's objection that Maine lacks regulatory authority over it related to any claims that may arise from this incident.

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

<<b2b\_text\_4(NOTICE OF DATA BREACH - CA Residents Only)>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

CNB Bank & Trust, N.A. values the relationship we have with our customers and understands the importance of protecting the personal information we maintain. We are writing to inform you of a data security incident involving our third-party service provider Fiserv that resulted in the disclosure of some of your personal information to an unauthorized actor. This letter explains the incident, measures that we and our third-party provider have taken, and some additional steps you may consider taking in response.

**What Happened?**

On <<b2b\_text\_2(date of incident)>>, we received a report from our third-party service provider for payment and financial services technology of an incident related to vulnerabilities discovered in MOVEit Transfer by Progress Software, the commonly used Managed File Transfer (MFT) software supporting file transfer activities by thousands of organizations around the world. Our service provider's investigation identified unauthorized activity in the service provider's MOVEit Transfer environment between May 27 and May 31, 2023, which was before Progress Software publicly disclosed the existence of this vulnerability. During that time, unauthorized actors obtained certain files transferred via MOVEit Transfer. **No CNB systems were involved in this incident.** Our service provider remediated the issue that led to the inadvertent disclosure and conducted a careful review of the files involved.

**What Information Was Involved?**

Based on that review, it was determined that one or more of the files contained <<b2b\_text\_3(name, data elements)>>.

**What We Are Doing.**

We wanted to notify you of this incident and to assure you that we take it seriously. To help prevent something like this happening again, our service provider remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. Our service provider also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities.

**What You Can Do.**

Our service provider has arranged for you to receive free identity monitoring services through Kroll for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Regardless of whether you elect to activate the free identity monitoring services, we strongly recommend that you remain vigilant and regularly review and monitor your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify CNB or any other of your financial institutions if you suspect any unauthorized activity.

**For More Information.**

For more information on steps you can take to protect your information, including instructions on how to activate your free identity monitoring services through Kroll, please review Attachments A and B that follow this letter. If you have any questions about this notice or the incident, please feel free to contact the dedicated incident response helpline at [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

<<b2b\_text\_1(Data Owner Name)>>

## ATTACHMENT A

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b\_text\_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s\_n>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).



### **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

#### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

#### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

#### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## **ATTACHMENT B**

### **ADDITIONAL STEPS YOU CAN TAKE**

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.identitytheft.gov](http://www.identitytheft.gov).

#### **Fraud Alerts and Credit or Security Freezes:**

***Fraud Alerts:*** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

***Credit or Security Freezes:*** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with 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.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

**Additional information for residents of the following states:**

**Connecticut:** You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag).

**District of Columbia:** You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, [www.oag.dc.gov](http://www.oag.dc.gov).

**Maryland:** You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us).

**Massachusetts:** Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html).

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov).

**Rhode Island:** **This incident involves XXX individuals in Rhode Island.** Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov).

**West Virginia:** You have the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active-duty military personnel have additional rights.