

Notice of Data Breach for the Maryland Attorney General

Nine Maryland residents will be notified. Attached to this Email you should find a copy of the template notification letter and a copy of the notification letter ABNB Federal Credit Union provided the NCUA, our regulator.

Summary of Incident:

On Wednesday, October 11, 2023, ABNB Federal Credit Union was notified by our core vendor Fiserv about a breach to an application hosted in their data center which resulted in a compromise of roughly 6,700 ABNB Federal Credit Union member account details. Analysis determined that number to be 3,800 ABNB Federal Credit Union member account details.

Incident Summary as delivered by Fiserv

On May 31, 2023, Progress Software, a Fiserv software service provider, disclosed a widespread zero-day SQL injection vulnerability in its MOVEit Transfer product that is having industry wide impact. MOVEit Transfer is a file sharing tool used across industries and governments. MOVEit Transfer is one of several file transfer tools that Fiserv uses. Fiserv took immediate steps to assess and respond to the situation, including swift patching of our production systems and heightened monitoring of the MOVEit Transfer environment. As part of those efforts, Fiserv wrote to your organization recommending that immediate steps be taken to change MOVEit Transfer account passwords. Fiserv also quickly activated its security response protocol and team, which includes a dedicated team of cybersecurity and forensics experts, alerted law enforcement, and began an investigation and review of potentially impacted data.

Analysis to date has revealed that certain data in Fiserv's MOVEit Transfer environment was exfiltrated between May 27 and 31, 2023, which was before Progress Software disclosed the existence of this vulnerability on May 31, 2023. The zero-day vulnerability exploit was likely carried out by a cyber-crime organization based in Russia. We are confident that our response to this vulnerability is aligned to industry practices and has addressed the vulnerability. We can confirm that this incident impacted only a limited number of the servers used for MOVEit Transfer. It did not impact any other Fiserv servers or systems. There was no evidence of lateral movement in our environment. We do not believe that any data exfiltrated from our MOVEit Transfer environment has been made available publicly or otherwise published to any unauthorized websites.

As a result of our ongoing investigation, Fiserv, together with our cybersecurity and forensic experts, have identified data belonging to your institution and we are writing to provide additional information about this.

files.

Our review has indicated that the files included the following data elements for some or all individuals: name, business name, address, state, telephone number, account number, and routing number. (end of Incident Summary as delivered by FiServ).

ABNB Federal Credit Union is in the process of notifying our impacted members. Fiserv has offered services to assist ABNB Federal Credit Union and its members through this event and will provide members that opt in with Experian Credit Monitoring, Fraud Consultation and Identity Theft Restoration.

Please contact me if you have any questions or require follow-up.

Kind regards,

Shawn Hayes

Director of Enterprise Risk Management and ISO | ABNB FCU

Serving Everyone in Hampton Roads and Northeastern NC

830 Greenbrier Circle
Chesapeake, VA 23320

www.abnbfcu.org

(O) – 757.523.5374



Statement of Confidentiality - This E-Mail and any attachments may contain confidential and privileged information. It is intended solely for the recipient(s) indicated. Any review, use, or distribution by anyone other than the intended recipient(s) is strictly prohibited. If you have received this E-Mail in error or are not the intended recipient, please notify the sender and delete all copies immediately

October 13, 2023

John Kutchey
Director, Eastern Region
National Credit Union Association
1775 Duke Street
Alexandria, VA 22314

VIA NCUA Zix E-mail

RE: NCUA Notification - ABNB Federal Credit Union Member Sensitive Data Compromise / Fiserv Breach

Dear Mr. Kutchey,

On Wednesday, October 11, 2023, ABNB Federal Credit Union was notified by our core vendor Fiserv about a breach to an application hosted in their data center which resulted in a compromise of roughly 6,700 ABNB Federal Credit Union member account details.

Incident Summary as delivered by Fiserv

On May 31, 2023, Progress Software, a Fiserv software service provider, disclosed a widespread zero-day SQL injection vulnerability in its MOVEit Transfer product that is having industry wide impact. MOVEit Transfer is a file sharing tool used across industries and governments. MOVEit Transfer is one of several file transfer tools that Fiserv uses. Fiserv took immediate steps to assess and respond to the situation, including swift patching of our production systems and heightened monitoring of the MOVEit Transfer environment. As part of those efforts, Fiserv wrote to your organization recommending that immediate steps be taken to change MOVEit Transfer account passwords. Fiserv also quickly activated its security response protocol and team, which includes a dedicated team of cybersecurity and forensics experts, alerted law enforcement, and began an investigation and review of potentially impacted data.

Analysis to date has revealed that certain data in Fiserv's MOVEit Transfer environment was exfiltrated between May 27 and 31, 2023, which was before Progress Software disclosed the existence of this vulnerability on May 31, 2023. The zero-day vulnerability exploit was likely carried out by a cyber-crime organization based in Russia. We are confident that our response to this vulnerability is aligned to industry practices and has addressed the vulnerability.

We can confirm that this incident impacted only a limited number of the servers used for MOVEit Transfer. It did not impact any other Fiserv servers or systems. There was no evidence of lateral movement in our environment. We do not believe that any data exfiltrated from our MOVEit Transfer environment has been made available publicly or otherwise published to any unauthorized websites.

As a result of our ongoing investigation, Fiserv, together with our cybersecurity and forensic experts, have identified data belonging to your institution and we are writing to provide additional information about this.

The files that belong to your institution relate to Item Processing Solutions services provided to your institution and may include check images, deposit slips, and remote deposit capture files.

Our review has indicated that the files included the following data elements for some or all individuals: name, business name, address, state, telephone number, account number, and routing number. (end of Incident Summary as delivered by FiServ).

ABNB Federal Credit Union is in the process of determining the best course of action on how to notify our impacted members. Fiserv has offered services to assist ABNB Federal Credit Union and its members through this event and will provide members that opt in with Experian Credit Monitoring, Fraud Consultation and Identity Theft Restoration.

We will provide you with an update once our incident response actions resulting from this issue has been completed entirely.

If you have any questions, please feel free to contact me at (757) 523-5739.

DocuSigned by:

16F22CA570F4481...

Charles A. Mallon, Jr.
President/CEO
ABNB Federal Credit Union

+

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Member Notification

We were recently notified by one of our technology service providers of a third-party data breach that impacted consumers across the country and that included some of our members. This was NOT a breach caused by ABNB but was a compromise of a limited number of account details on *their* system. This compromise may have affected you. *Importantly, our review of their analysis of this issue did not identify any evidence of fraud related to your account.*

As soon as we were made aware of this incident, we took immediate action requiring the vendor to conduct a comprehensive investigation to identify any ABNB members who were affected. We wanted to notify you of this incident and to assure you that we take the security of our members' information very seriously and we require our business partners to do the same.

Next Steps

Although our service provider's investigation has found no evidence of fraud on your account, you can receive free identity monitoring services for two years through a trusted company named Kroll.

Kroll is a global leader in monitoring these consumer issues and has extensive experience helping people who may have had limited exposure of confidential data.

Kroll's free identity monitoring services are available to you right now and include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

If you have any questions about this incident, please call Kroll directly at 866.731.2928, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. They will answer your questions and help you get started with their free identity monitoring services for your account.

Rest assured, we will continue to closely monitor this situation, including requiring regular updates on our technology service provider's investigation and findings. Please see the attachments to this letter for more detailed information on the identity monitoring services available to you at no cost. Thank you for being a member. We appreciate your business.

Sincerely,

The ABNB Information Security Team

P.S. As always, if you notice any suspicious transactions on your account, or something doesn't look right to you, please contact us immediately for assistance.



NOTICE OF THIRD-PARTY DATA BREACH

We are contacting you regarding an incident involving the MOVEit Transfer software. This incident has caused the potential disclosure of some of your personal information to a third party. On October 11, 2023, one of our technology service providers made us aware of an incident related to vulnerabilities discovered in the MOVEit Transfer software by Progress Software, a commonly used secure Managed File Transfer (MFT) software supporting file transfer activities by thousands of organizations around the world. The MOVEit Transfer software was used by our technology service provider to support a subset of the services we provide to our members.

Our vendor's analysis, to date, has identified unauthorized activity in the MOVEit Transfer environment between May 27 to 31, 2023, which was before Progress Software publicly disclosed the existence of this vulnerability. During that time, unauthorized actors obtained files transferred via MOVEit Transfer which included certain personal information.

What Information Was Involved?

From their review of the contents of the files, it was determined that one or more of the files may have contained personal information including <<b2b_text_3 (your name, impacted data elements)>>.

What Are We Doing?

We wanted to notify you of this incident and to assure you that we take it seriously and we require our business partners to also take this seriously. What we currently understand is that upon learning of this incident, the IT service provider took immediate steps to launch a comprehensive investigation, identify individuals affected and notified regulatory bodies as required. To help prevent something like this happening again, our service provider has remediated their known 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.

We have arranged for you to receive a complimentary free identity monitoring service 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.

For more information on identity theft prevention, including instructions on how to activate your identity monitoring, as well as some additional steps you can take for your protection, please review Attachments A and B that follow this letter.

Regardless of whether you elect to activate the identity monitoring service, we strongly recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify us or any other of your financial institutions if you suspect any unauthorized activity. In addition, we suggest that you change any passwords associated with your accounts.

If you would like to open a new account as an extra safety precaution, please contact us directly at 757.523.5300

For More Information.

Please be assured that we are taking steps to address the incident and to help protect the security of your data. If you have any questions about this notice or the incident, please feel free to call 866.731.2928, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

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.



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

To help protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus.

To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:

Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might help protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to help protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

District of Columbia Residents: The Attorney General can be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or <https://oag.dc.gov/>.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or <http://www.ncdoj.gov>.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Avenue, Albany, NY, 12231-001, (518) 474-8583/(800) 697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY, 12224-0341, (800) 771-7755, <https://ag.ny.gov>.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or <http://www.riag.ri.gov/>. You may also file a police report by contacting local or state law enforcement agencies.