PISCATAQUA SAVINGS BANK

piscataqua.com

15 Pleasant Street
Portsmouth, NH 03801
(603)436-5250

If you received a letter from Piscataqua Savings Bank or Kroll, please read the information Below.

A recent security incident that impacted numerous companies worldwide, including one of the vendors whom Piscataqua Savings Bank utilizes for processing transactions. This post is meant to provide you with details on the incident that occurred, and measures taken in response to the incident as well as to provide you with information on steps you may consider taking to further protect your personal information.

What happened?

On May 31, 2023, Progress Software Corporation announced a previously unknown vulnerability affecting its MOVEit Transfer application. MOVEit is a file transfer software used worldwide to transfer data between businesses. The vendor used by Piscataqua Savings Bank to initiate the processing of transactions was impacted by this incident. During the time of the vulnerability, unauthorized parties obtained files transferred via MOVEit. Piscataqua Savings Bank has been assured by the vendor that the issue has been contained and that the vulnerability has been remediated. A technical response team was also mobilized at this time to examine the transfer system and ensure that there are no further vulnerabilities in the system. As an important note, this was not a targeted attack, but worldwide affecting the government, technology, and healthcare industries.

What does this mean for Piscataqua Savings Bank customers?

Our team at Piscataqua Savings Bank was made aware of the MOVEit vulnerability on Thursday, August 3rd and immediately began working with our vendor to obtain additional information about the incident. It was confirmed that the account numbers, addresses, birthdays, and social security numbers of affected customers were compromised. **NO** online banking usernames or passwords were accessed by unauthorized parties.

What you can do.

Piscataqua Savings Bank recommends that all customers regularly monitor their account(s) for suspicious activity. To facilitate this, we have arranged for our customers to receive two years of complimentary identity monitoring, including: Credit Monitoring, Fraud Consultation, and Identity Theft Restoration through Kroll. Kroll is a global leader in risk mitigation and response and their team has extensive experience helping those who have sustained unintentional exposure of confidential data.

Regardless of whether you elect to activate the identity monitoring service, we strongly recommend that you remain vigilant and regularly review 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 of your other financial institutions if you suspect unauthorized activity.

Piscataqua Savings Bank takes great pride in having served many generations of our Seacoast community. Our relationship with you, our customer, and the security of your account are our highest priority. Even though this breach happened though a 3rd party, your information is our responsibility and have taken steps internally to add additional safeguards to your accounts.

Breach Timeline of Events:

1. A file transfer software, the MOVEit Transfer application, used by thousands of companies across the world and multiple industries including government, healthcare finance and technology companies was compromised by a Russian hacking group.

2. Our Financial software vendor was one of the companies affected by this security breach. This was not targeted at Piscataqua Savings Bank.

3. Upon investigation, the data protection was configured correctly by being encrypted, but the zero-day vulnerability **(which means it was exploited before a patch was made available)** discovered by this hacking group gave administrator access to this software.

4. The MOVEit Transfer environment was exfiltrated between May 27 and 31, 2023. Progress Software disclosed the existence of this vulnerability on May 31,2023 and a zero-day vulnerability patch was issued and applied to the affected servers.

5. Cybersecurity experts and forensic investigators have been working since to identify what information was compromised.

6. During the time of the vulnerability, unauthorized parties obtained files transferred via MOVEit. The Bank was made aware that some information from some (but not all) of our customers were compromised on Thursday, August 3rd and we immediately began working with the vendor to obtain additional information about the incident.

7. It was confirmed that account numbers, addresses, birthdays, and social security numbers were affected.

Frequently Asked Question:

I don't have my credit monitoring credentials from Kroll yet... What can I do?
The credentials were mailed on 10/26/23. Below is information on how to Freeze or Lock credit with all 3 credit bureaus. This can be done both over the phone and online.

Why does the Bank need my Social Security Number?
2 reasons – Bank Secrecy Act/ USA PATRIOT Act requirements for customer Identification reasons.
And IRS = to file 1099 int 1098 and other various forms require by IRS.

Why am I just learning about this breach now when it happened on May 31st?
This Breach affected Progress Software Corporation who owns the software MOVE-it (a file transfer program used by thousands of businesses). The forensic investigation at Progress
Software started once they were aware of the Breach but had to comb though thousands of files from thousands of companies.

Some companies have been alerted before us, and the investigation is still in process as other companies have not been notified or discovered yet as this is an ongoing investigation.

Whose fault was this?
In short, a Russian Hacking group called KLOP. The customer information breached was protected and encrypted as it should have been. KLOP had been working for 2 years testing ways to infiltrate the MOVE-it software and ultimately found a way in with administrator access – so it didn't matter the file was encrypted. (For more information – see https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/

Why was my information on the MOVEit Server?
It is a state required file to the NH Department of Child Services that is transferred from our core provider on a monthly scheduled basis. Although the file was encrypted in transit – the attacker had elevated authority to extract and decrypt the file.

Was that the only information in that file?
The file included: Account number, Primary name, Secondary Name, address, City, state, zip, date of birth, account balance (rounded), account number and Tax ID.

The Credit Monitoring is only for 18 and over – what if my child was on the compromised list?
Credit reports for minors who are 13 years of age or under cannot be accessed online because the Children's Online Privacy Protection Act restricts the online collection of personal information regarding children.

Equifax

A cover letter must be sent requesting a security freeze be put on child's account under the age of 18. Included with that cover letter there must a copy of the child's birth certificate, social security card, and a copy of a parent's drivers licenses. The mailing address is:

Equifax Security Freeze
PO Box 105788
Atlanta, Georgia 30348

Experian

https://www.experian.com/help/minor-request.html This link is very helpful and has everything you need for kids 14 and older and what to do with 13 and under.

Requesting a Minor's Credit Report, Fraud Alert or Security Freeze

Experian does not knowingly maintain credit information on minors in our database. If you are a minor who is 14 years old or older, you may request a copy of your personal credit report, add a fraud alert or place or remove a security freeze by using this web site or by writing to us. We will either process your request or notify you that we do not have credit information about you. Credit reports for minors who are 13 years of age or under cannot be accessed online because the Children's Online Privacy Protection Act restricts the online collection of personal information regarding children. Parents of minors 13 years of age or under who want to know if Experian's database contains credit information about their child may write to us.

Transunion

Below is the response we received from Transunion regarding credit freeze for minors.

We received your inquiry regarding **minor children.** We take your concern and all identity theft seriously. We're here to help.

We're happy to process your request, but we will need more information from you. Please submit your request through our secure online Child Identity Theft Inquiry Form using the link below:

https://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/childIDInquiry.page

You may also send your request by mail to:

TransUnion
P.O. Box 2000
Chester, PA 19016

Please provide the following information with your request:

- Proof of minor child's identification, provide one of the following:
  - Social Security Card
  - Certified copy of birth certificate
  - Driver's license
- Proof of authority (documentation demonstrating that you can act on behalf of the minor child), provide one of the following:
  - Court order
  - Valid Power of Attorney
  - Proof of parentage, including birth certificate
  - County welfare department for foster care consumer

If you have any additional questions or would like to speak to a representative, please call 800-916-8800.

14 and over:
Children 14 and older can check their credit the same way as adults.

ADDITIONAL STEPS YOU CAN TAKE

- Setup alerts though your Online Banking portal. For more information please visit: https://www.piscataqua.com/deposits/online-banking/ealerts/

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:	Experian:	TransUnion:
Equifax Information Services LLC	Credit Fraud Center	Fraud Victim Assistance Department
P.O. Box 105788 Atlanta, GA 30348	P.O. Box 9554 Allen, TX 75013	P.O. Box 2000 Chester, PA 19022-2000
1-888-298-0045	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	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 ca be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.