EXHIBIT 1

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Kearny Bank does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

This event occurred at Fiserv, a third-party vendor that provides Kearny Bank with financial technology services. It did not involve any Kearny Bank systems or applications and is not the result of any action or inaction on Kearny Bank's part. All Kearny Bank systems, including its core banking systems, remain secure and were not impacted by this event.

To support the products and services that Kearny Bank provides to its customers, Fiserv utilizes a Managed File Transfer (MFT) tool known as MOVEit Transfer. On August 8, 2023, Fiserv notified Kearny Bank that the zero-day vulnerabilities publicly disclosed by Progress Software Corp. in May and June of 2023 impacted Fiserv's instance of the MOVEit Transfer tool. Specifically, Fiserv notified Kearny Bank that between May 27, 2023 and May 31, 2023, an unauthorized actor gained access to Fiserv's MOVEit Transfer environment and obtained certain files contained therein, including files that it maintains for Kearny Bank.

Upon being notified by Fiserv, Kearny Bank launched its own investigation and worked with Fiserv to confirm the nature and scope of information potentially impacted and to identify the individuals to whom such information relates. On September 25, 2023, Fiserv provided Kearny Bank with data and information which allowed Kearny Bank to identify the specific Kearny Bank clients impacted. The personal information related to Maine residents affiliated with Kearny Bank that could have been subject to unauthorized acquisition include the following: name, address, and financial account information.

Notice to Maine Residents

On October 25, 2023, Fiserv, on Kearny Bank's behalf, began providing written notice of this event to potentially impacted individuals affiliated with Kearny Bank, including approximately three (3) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon being notified of the event, Kearny Bank moved quickly to investigate and respond to the Fiserv event, assess the security of Kearny Bank's own systems, confirm the nature and scope of information potentially impacted, and identify the individuals to whom such information relates. Fiserv, on Kearny Bank's behalf, also is providing access to credit monitoring, fraud consultation, and identity restoration services for twenty-four (24) months, through Kroll, to individuals whose personal information was potentially affected by the Fiserv event, at no cost to those individuals.

Additionally, Fiserv, on Kearny Bank's behalf, is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report

any suspected incidents of identity theft or fraud to their applicable financial institution. Fiserv, on Kearny Bank's behalf, is providing individuals with information on how to place a fraud alert and credit freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Kearny Bank is providing written notice of this event to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

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

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

<<b2b_text_2(Notice of Data Breach - CA residents only)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of an event that may affect the security of some of your personal information. This event occurred within the systems of one of our third-party vendors, a Fortune 500 company, and not within our internal systems. The event had no impact on our systems and was not the result of any action or inaction on our part. Although we are unaware of any actual misuse of your information, we are writing to provide details about the event, our response, and resources available to help protect your personal information from possible misuse.

What Happened?

Our third-party vendor, and thousands of other organizations around the world, utilize secure Managed File Transfer software provided by Progress Software Corp. ("Progress Software"), known as MOVEit Transfer. Our third-party vendor utilizes MOVEit Transfer to support various products and services that its clients, including Kearny Bank, use.

On May 31, 2023, and again in June 2023, Progress Software publicly disclosed vulnerabilities that impacted MOVEit Transfer, including our third-party vendor's version of MOVEit Transfer. Our third-party vendor launched an investigation and determined that between May 27, 2023 and May 31, 2023, prior to Progress Software's public disclosure, an unauthorized party gained access to our third-party vendor's MOVEit Transfer systems and obtained certain data files, including files that are maintained for Kearny Bank. Our third-party vendor also notified law enforcement regarding this event. On August 8, 2023, our third party vendor notified us that Kearny Bank was affected by this event. On September 25, 2023, our third-party vendor provided us with data and information which allowed us to identify the specific Kearny Bank clients impacted.

What Information Was Involved?

Our investigation determined that files containing your <<b2b_text_3(name, data elements)>> were potentially obtained during the event.

What We Are Doing.

Upon learning of this event from our third-party vendor, we took immediate steps to launch a comprehensive investigation, identify clients impacted, and notify the applicable regulatory bodies, as required. Concurrently, our third-party vendor remediated all technical vulnerabilities in accordance with Progress Software's guidelines and mobilized a technical response team to ensure that there were no further vulnerabilities.

What You Can Do.

We have arranged for you to receive complimentary identity monitoring through Kroll for two years. Kroll is a global leader in risk mitigation and response and their identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Regardless of whether you elect to enroll in the identity monitoring service, we recommend that you remain vigilant and regularly monitor your account activity and credit history to guard against any unauthorized activity.

For more information on identity theft prevention, including instructions on how to enroll in complementary identity monitoring, please review Attachments A and B that follow this letter.

For More Information.

If you have any further questions please feel free to contact us 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.

KROLL

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:	Experian:	TransUnion:
Equifax Information Services LLC	Credit Fraud Center	Fraud Victim Assistance Department
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-888-298-0045	1-888-397-3742	1-800-916-8800
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 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. This notice has not been delayed by law enforcement.

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 276999001; (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. The New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or 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.