



◆ THE "COMMUNITY" BANK THAT PUTS PEOPLE FIRST ◆

Member FDIC

September 21, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Office of the Attorney General,

On August 18, 2022, Josh Bopp, President of FocusIT communicated to Chris Oswald, E.V.P.-Chief Operations Officer/Information Technology (IT) Security/Compliance Officer of Farmers and Merchants Bank, of a breach occurrence impacting the hosted customer database of the Farmers and Merchants Bank Mortgage Division on August 2, 2022. FocusIT, is a third-party vendor of the Farmers and Merchants Bank's Mortgage Division responsible for hosting the Calyx Point mortgage origination and loan processing software application. FocusIT was notified by the Texas Financial Crimes Intelligence Center on August 2, 2022, that an unknown threat actor(s) potentially compromised a third party system, Hightail, Inc. affecting the secure database records hosted by FocusIT.

FocusIT, [REDACTED] to perform a comprehensive investigation and review of the reported breach occurrence. [REDACTED]

[REDACTED] Their review indicated on Monday, July 25, 2022, a threat actor(s) posted & displayed login credentials of a FocusIT employee, possibly compromised through a phishing email, on the dark web for \$ 300 in payment. [REDACTED]

[REDACTED]

In review of the [REDACTED] Listing of customer database records for the Farmers and Merchants Bank's Mortgage Division, approximately 5,300 individual customers are potentially at risk of compromise of personal information including Tax ID Numbers (SSN). FocusIT has prepared a letter of notification to each impacted customer and provided to the senior management of Farmers and Merchants Bank for their review and approval, authorized by Farmers and Merchants Bank on September 9, 2022. Each letter of notification outlines the forensics investigation review, description of Equifax Credit Monitoring services extended to the individual at no cost, contact information for reporting consumer Fraud Alerts, and information on security freezes with credit bureaus if desired by the individual.

In reporting this information, Farmers and Merchants Bank regrets the occurrence of the data breach by its third-party vendor, FocusIT, affecting customers of the bank's Mortgage Division. Farmers and Merchants Bank discontinued third-party services with FocusIT in July 2022 [REDACTED]

Main Office
15226 Hanover Pike
Upperco, MD 21155
(410) 833-6600
FAX (410) 526-3835

Hampstead Branch
735 Hanover Pike
Hampstead, MD 21074
(410) 239-4448
FAX (410) 374-4240

Greenmount In-Store Branch
2320 Hanover Pike
Hampstead, MD 21074
(410) 374-3436
FAX (410) 374-3756

Reisterstown Branch
25 Westminster Pike, PO Box 249
Reisterstown, MD 21136
(410) 517-3060
FAX (410) 517-3061

Owings Mills Branch
9320 Lakeside Blvd.
Owings Mills, MD 21117
(410) 356-8200
FAX (410) 356-5456

Westminster Branch
275 Clifton Blvd.
Westminster, MD 21157
(410) 857-1100
FAX (410) 857-2360

Eldersburg Branch
1321 Liberty Road
Sykesville, MD 21784
(410) 795-1900
FAX (410) 549-1715



◆ *THE "COMMUNITY" BANK THAT PUTS PEOPLE FIRST* ◆

Member FDIC

Farmers and Merchants Bank maintains stringent Information Technology (IT) security and compliance practices in protection of all computer network systems and software applications in accordance with the Federal Financial Institutions Examination Council (FFIEC) industry standards. Annually, Farmers and Merchants Bank contracts an independent Information Technology (IT) Security Audit Consultant to perform a comprehensive (IT) Risk Assessment of the bank's network security infrastructure, systems, and applications in accordance with NIST Cybersecurity Framework guidelines for mitigation of cybersecurity risks. From the implementation date of the bank's computer network on September 30, 2002, there have been zero (0) occurrences of data breaches to any of Farmers and Merchants Bank's computer systems, software applications, and stored databases to the current date of September 20, 2022.

Thank you for your assistance in this matter, and please feel free to contact me if you should have any questions or concerns at 410-374-1510 X 107 or via email correspondence to: chris.oswald@fmb1919.bank.

Respectfully Submitted,

Christopher T. Oswald

Executive Vice President-Chief Operations Officer
Information Technology (IT) Security/Compliance Officer

Main Office
15226 Hanover Pike
Upperco, MD 21155
(410) 833-6600
FAX (410) 526-3835

Hampstead Branch
735 Hanover Pike
Hampstead, MD 21074
(410) 239-4448
FAX (410) 374-4240

Greenmount In-Store Branch
2320 Hanover Pike
Hampstead, MD 21074
(410) 374-3436
FAX (410) 374-3756

Reisterstown Branch
25 Westminster Pike, PO Box 249
Reisterstown, MD 21136
(410) 517-3060
FAX (410) 517-3061

Owings Mills Branch
9320 Lakeside Blvd.
Owings Mills, MD 21117
(410) 356-8200
FAX (410) 356-5456

Westminster Branch
275 Clifton Blvd.
Westminster, MD 21157
(410) 857-1100
FAX (410) 857-2360

Eldersburg Branch
1321 Liberty Road
Sykesville, MD 21784
(410) 795-1900
FAX (410) 549-1715



September [redacted], 2022

[Individual's Address]

Re: NOTICE OF DATA BREACH

Dear [Individual]:

We write to inform you of a recent incident that may have involved personal information about you.

WHAT HAPPENED? On August 2, 2022, focusIT, Inc. was notified by the Texas Financial Crimes Intelligence Center that unknown threat actor(s) potentially compromised a third party system in the focusIT environment. FocusIT is a third party vendor of the Farmers and Merchants Bank who facilitates Residential Mortgage application processing. This compromise resulted in your personal information potentially being downloaded by unknown threat actors. This incident was swiftly investigated and contained.

WHAT INFORMATION WAS INVOLVED? Personal information of some [insert focusIT business customer] account holders including name, address, Social Security number, and [date of birth].

WHAT WE ARE DOING. As a victim of this crime, we are working with the appropriate law enforcement and regulatory officials including the FBI. Please know that protecting your personal information is something that we take very seriously. We apologize for both this unfortunate incident and any inconvenience it may cause you. We are providing notice and offering credit monitoring services to certain individuals based on the personal information that was potentially exposed. Nevertheless, there are important steps that you can take to reduce the potential risk of identity theft or fraud.

WHAT YOU CAN DO. If you provided your account and password information in a message, please change your password at all sites where you use the same password. We further recommend avoiding easy-to-guess passwords. You should be on guard for identity theft schemes and phishing where malicious actors may pretend to represent us or reference this incident. If you have questions, please contact us at the number described below.

To help protect your identity, we are offering a **complimentary** credit monitoring services as described below. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. If you believe your personal information was affected, please contact us so that we may pursue our investigation to the fullest extent of the law. In addition the following website by the National Cyber Security Alliance offers inciteful tips to protect yourself online. <https://staysafeonline.org/resources/online-safety-privacy-basics/>



OTHER IMPORTANT INFORMATION. The Federal Trade Commission (FTC) recommends that you remain vigilant by checking your credit reports periodically. Checking your credit reports can help you spot problems and address them quickly. You can also order free copies of your annual reports through www.annualcreditreport.com. You should monitor your financial accounts for any suspicious activity. For more information about steps you can take to reduce the likelihood of identity theft or fraud, call 1-877-ID-THEFT (877-438-4338), visit the FTC's website at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>, or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. However, if you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state's attorney general, or the FTC.

Credit Monitoring Instructions

We have arranged for you to receive free credit monitoring to help you protect your identity and credit information. (See enclosed instructions.) If you choose to enroll, you will receive communications detailing any key changes to your credit reports. To enroll, you will also need the Promotional Code provided below. Your coverage will last for 12-24 months from the date of enrollment depending on the state where you live.

Website enrollment: [Equifax URL]
Your Promotional Code: XXXXX

Contact Information for Consumer Reporting Agencies and Information on Credit Report Fraud Alerts

You may also choose to place a fraud alert on your credit file, which is free of charge to you and can be done with any *one* of the companies listed below (i.e., if you place a fraud alert with one company, they will automatically notify the others). A fraud alert tells creditors to contact you *before* they open any new accounts or change your existing accounts.

	Experian	Equifax	TransUnion
Phone	1-888-397-3742	1-800-525-6285 or 1-888-766-0008	1-800-680-7289
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division PO Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report	https://www.experian.com/fraud/center.html	https://www.equifax.com/personal/credit-report-services/	https://fraud.transunion.com/fraudAlert/landingPage.jsp



Fraud Alert Form			
---------------------	--	--	--

Information on Security Freezes

In addition to a fraud alert, you may place a security freeze on your credit file. A security freeze **will block** a credit bureau from releasing information from your credit report without your prior written authorization. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. The fees for placing a security freeze vary by state, and a consumer reporting agency may charge a fee of up to \$10.00 to place a freeze or lift or remove a freeze.

To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online.

	Experian	Equifax	TransUnion
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	https://www.experian.com/freeze/center.html	https://www.equifax.com/personal/credit-report-services	https://www.transunion.com/credit-freeze

You may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes.

FOR MORE INFORMATION. If you have any questions, please feel free to call 1-800-###-####. We sincerely regret that this incident occurred.

Sincerely,

focusIT Security Team



State-Specific Information

If you are a resident of the following states, the following information applies to you.

For residents of Maryland, New York, North Carolina, Rhode Island, the District of Colombia: For information on how to avoid identity theft or to contact your state's attorney general, please use the below information.

Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
1 (888) 743-0023 https://www.oag.state.md.us/ Attorney General of Maryland 200 St. Paul Place Baltimore, MD 21202	1-877-566-7226 http://www.ncdoj.gov Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001	(401) 274-4400 http://www.riag.ri.gov/ Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903
District of Columbia Attorney General	New York Attorney General	
(202) 727-3400 https://oag.dc.gov Office of the Attorney General for the District of Columbia 441 4th St. NW Washington, DC 20001	1-800-771-7755 https://ag.ny.gov/ Office of the Attorney General The Capitol Albany, NY 12224-0341	

For residents of New Mexico: You have rights under the federal Fair Credit Reporting Act (FCRA). These include: the right to access information in your consumer file at a consumer reporting agency; to dispute incomplete or inaccurate information in your consumer file at a consumer reporting agency; to have consumer reporting agencies correct or delete inaccurate information in your consumer file; the right to block information in your consumer file that is the result of identity theft; and the right to have a fraud alert placed on your consumer file (as described above). For more information, please visit <https://www.consumer.ftc.gov/> or <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

For residents of Rhode Island: Under Rhode Island law, you have the right to obtain a police report filed in regard to this 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.

Based on our investigation to date, we believe this incident affected the personal information of fewer than ### individuals in Rhode Island.