



I would like to inform you of a notification incident that occurred at MainStreet Bank. We have identified unauthorized access of a third-party system that occurred between October 24th 2022 02:48 UTC and November 1st 2022 15:00 UTC. We have disabled the suspicious accounts, forced password changes of all employee accounts in this system, and made additional account and security changes to the platform to reduce the possibility of future account compromise.

This system contains a small subset of customer records and is totally isolated from our Core system. We have currently identified 23 suspicious IP addresses, 10 compromised user accounts, 121 suspicious web requests, and 38 documents related to this incident.

We will be sending breach notifications to 80 individuals, 14 of which have Maryland addresses listed as their residence address. Please let me know if you require any additional information. Thank you.



Matt McCrory

SVP, Chief Information Security Officer

(703) 481-4551 Direct

(703) 994-6620 Cell

mmccrory@ mstreetbank. com

www.mstreetbank.com

www.venu.bank

[share your feedback](#)

Dear {Customer Name},

We are writing to notify you of an incident involving one of our third-party systems in which some of your personal information may have been exposed. Although we are unaware of any actual compromise or misuse of your information, we are informing you and other potentially affected customers about the incident to assist you in protecting yourself against possible identity theft or fraud.

On October 31, we identified unauthorized access to one of our third-party database systems. Upon discovering the unauthorized user, we immediately identified the method of entry, removed the intruder, and reported the matter to our federal regulator, the Federal Reserve Bank of Richmond.

Information that the intruder may have accessed includes names, addresses, phone numbers, and social security numbers. No online account information or passwords were stored in the affected database.

As a precaution, we would like to offer you one year of credit monitoring and identity protection services with LifeLock.

You may also choose to place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies listed below:

Equifax (888)766-0008 or www.fraudalert.equifax.com

Experian (888) 397-3742 or www.experian.com

TransUnion (800) 680-7289 or www.transunion.com

Safeguarding customer information is key to our role as a financial institution. We have long made significant investments in cybersecurity and will continue to do so. We are incorporating the lessons from this incident to further strengthen our cyber defenses.

If you have any questions or would like to enroll in credit monitoring, please contact [your Business Banker or Relationship Manager] OR [Debra Cope, MainStreet Bank's Head of Corporate Communications] to facilitate the request.