May 4, 2021

In late March, U.S. Bank was subject to a credential stuffing event. In this event, the hackers successfully used stolen username and passwords to access approximately 340 customer accounts. This was not a breach of U.S. Bank systems, however customer account numbers may have been viewable. The hackers took information stolen from other sites and used them to attempt logins on U.S. Bank’s systems. To date, no fraudulent transactions related to this event have been identified on these customers’ accounts. We have contacted all impacted customers to ensure they change their username and password or close their account. The privacy and security of our customer’s information is our top priority and we worked quickly to prevent the use of stolen data to access our customers’ accounts.

The bank maintains a notification plan designed to meet the requirements of the Gramm Leach Bliley Act and notified its customers in accordance with that plan. The email message below was sent to all customers potentially affected. The bank called customers whose information we believed was accessed. In those calls, bankers discussed the nature of the event and what information was affected, and reviewed account transactions with the customers. The small number of customers who could not be reached by phone after multiple attempts were sent a letter with additional information about the event. That letter is provided separately.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|

|  |  |
| --- | --- |
|  |  |

 |

 |
|

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|

|  |  |
| --- | --- |
| U.S Bank |  |

 |

 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
|

|  |  |
| --- | --- |
|

|  |
| --- |
| The security of your information is a top priority for U.S. Bank. We recently noticed some suspicious log in attempts that may impact your account. **As a precautionary measure, we have locked your Online Banking account and are asking you to reset your password**. To reset your password, visit the app or go to usbank.com and click “Get login help.” We also encourage our customers to monitor their financial accounts closely on a regular basis. Here are some steps you can take to protect yourself from fraudulent activity on your accounts: * When resetting your password, it’s recommended to choose a unique password and not one that has been used previously.
* U.S. Bank will never initiate a request for your sensitive information like your Personal ID, Password, Social Security Number, Personal Identification Number (PIN) or Account Number. For your safety, never share this information with anyone, at any time.
* Monitor your accounts regularly and watch for unusual transactions.
* Activate fraud watches, email and text alerts on all accounts (checking, saving, credit cards) to help spot unusual transactions quickly.
* Read security alerts when you receive them. U.S. Bank will send a security alert when certain changes are made to your account—pay attention to these, they are designed to help identify fraud quickly.
* Leverage two factor authentication (i.e.: register your mobile number), whenever available. By using this type of authentication process, you reduce the likelihood of someone being able to fraudulently change or access your account.

**We are always here to assist**. Please contact us at 800.USBANKS (800.872.2657) if you have any questions or identify any suspicious activity on your account.   |

 |

 |

 |

 |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|   | Facebook |   | Twitter |   | Instagram |   | [**Get the app**](http://link.notifications.usbank.com/ls/click?upn=uaTXP6-2BZzqWW7gDVhy78MYfqlSxxrtG4mErPZoiAqwfZeoLaKwJLTADLmyj3nfO0-2BG8X7fB4yqjXViSqvqAfVjd5rPUFOUnZrhI72jEYCYg-3DNdz9_WdEosL0DLIaXUW6MaAMZRDVmYnp8wed1slsv5J34ZZ7WUONbHjYfl-2FFf6Dx-2BssiX2YES1VrLIF-2BB7OnCYKdu8BXsqk01mWNYyIwpbyhmMfpprLTHBx95b6RK97c46MoXVm6lVkxEzZ8tAjEttt0jZ8T0DoE4RUA8cNytmDLwSyOysAsTOFsnhXYlvIVUBvpvvRvNCmPbxtTEp2M1mDMyyBz85t-2BMZKU4EaWfUtpLFiiXxG9n5ehJ-2B5kVv7TKbyRdOGba7MI1Lf9r-2BoeN2Vse7ln-2B0Ag3EzWCbTD98anrGKdVmQ3KzAXVpiL1H4g6aoMhe7cOBTn0X8gRZY-2Fc6qF-2FI-2BOIw2p-2BpGCbNe8HouooFzgOqZ3eBMGXFuCtb6t1wCiJecWQKZ5Bx8PU-2B6NaFR9r6Q-3D-3D)  |   | Mobile App |   |

 |

 |

 |

 |
|

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Email intended for: sumedh.nandedkar1@usbank.com

|  |  |  |
| --- | --- | --- |
|   |  |   |
|   |   |
|   |   |

Protecting your privacy is our priority. We'll never initiate a request via email for your sensitive information like your Personal ID, Password, Social Security Number, Personal Identification Number (PIN) or Account Number. For your safety, never share this information with anyone, at any time. If you receive an email asking for your sensitive information, or would like to report a suspicious email, forward it to fraud\_help@usbank.com or call U.S. Bank Customer Service immediately at 800.USBANKS (872.2657).[Get more details](http://link.notifications.usbank.com/ls/click?upn=uaTXP6-2BZzqWW7gDVhy78MYfqlSxxrtG4mErPZoiAqwfJdHHszYgMaUACne70YX5pTK1KHd9tDk3GCPORw3mnq4U5l816p1fxIbtYZGSkhaI-3DZ6B4_WdEosL0DLIaXUW6MaAMZRDVmYnp8wed1slsv5J34ZZ7WUONbHjYfl-2FFf6Dx-2BssiX2YES1VrLIF-2BB7OnCYKdu8BXsqk01mWNYyIwpbyhmMfpprLTHBx95b6RK97c46MoXVm6lVkxEzZ8tAjEttt0jZ8T0DoE4RUA8cNytmDLwSyOysAsTOFsnhXYlvIVUBvpvTMIgnjIBbh-2FGRpWGYAE9xymCRylj5Q3Jnql01u1P-2Fnnji-2B2e6j4TS8Sdx7QQKYs5V3hhgF8GXe0iRs9AY9eHicap0fiRrwivQlQ8DY3CgU5GsxpUZgFI3w0Uw3-2BzKNEEIYOfvHux3HwVE8szKJn716FsL7OborXVtkMBoJk-2FiwW4pcI-2BboGJtdrz0XCtxAPk-2BpNxDtaEIe9ylzvJxWmkOw-3D-3D) about recognizing online fraud issues.**Note:** If you'd rather not follow links from this email, you can access information on all U.S. Bank products and services at [usbank.com](http://link.notifications.usbank.com/ls/click?upn=uaTXP6-2BZzqWW7gDVhy78MRiVAcf3c9AgUIrEbwS4qtA-3Df0F1_WdEosL0DLIaXUW6MaAMZRDVmYnp8wed1slsv5J34ZZ7WUONbHjYfl-2FFf6Dx-2BssiX2YES1VrLIF-2BB7OnCYKdu8BXsqk01mWNYyIwpbyhmMfpprLTHBx95b6RK97c46MoXVm6lVkxEzZ8tAjEttt0jZ8T0DoE4RUA8cNytmDLwSyOysAsTOFsnhXYlvIVUBvpvPAirtTWwsF5Gt-2FHoSaEfss5Q6MqSWzsbdK8zkOyD-2Fg5ClhOjlQ8pJKmmBbCXfqai5Rx-2FjyP7BNkJR1R5HH3TW6yQqkxfc8xlCytHq8CwZOtwf6jn56kQ7mKm5-2FPwEpJ7WESiQ5DJdl3WqH41MBrQqYfsiYiFzdOuE1ddsLFNiTb9uitrTazE-2F9B0pGQ6NxkIndYcsmx84rBjcJfKTuyVrg-3D-3D).To ensure that you continue to receive email from us, please add us to your Address Book ([1800USBanks@email.usbank.com](1800USBanks%40email.usbank.com)). Thank you.You are receiving this email as a service to your account because you are a U.S. Bank customer.[View](http://link.notifications.usbank.com/ls/click?upn=uaTXP6-2BZzqWW7gDVhy78MYfqlSxxrtG4mErPZoiAqwdvo6X33ZjYCoJnalgWwY1cCaZs_WdEosL0DLIaXUW6MaAMZRDVmYnp8wed1slsv5J34ZZ7WUONbHjYfl-2FFf6Dx-2BssiX2YES1VrLIF-2BB7OnCYKdu8BXsqk01mWNYyIwpbyhmMfpprLTHBx95b6RK97c46MoXVm6lVkxEzZ8tAjEttt0jZ8T0DoE4RUA8cNytmDLwSyOysAsTOFsnhXYlvIVUBvpvcu6r8WWvNSLQ-2BO7c5nEz6PfpEVIwbL1hk3AVm9-2FG2sdp-2FogToQqB-2FnxfhPVoYtzMI3zMRw6mZV7X9gJJzilMqxLF0Wof4KNLzAfKVQDDAIaGVJ4cH4-2FIWWQTtHbEHR42WIi7FSIRusd-2BAzIC1YJ6bzmwTRa2gM4frbv3wY3GoaG7KIKCZEB565CUMTXKKfLT7TgKoECGoUPhinPD5BO3Ia5UfeOxx5rXd0plo0rvn-2BM-3D) the U.S. Bank Privacy Pledge.U.S. Bank, EP-MN-L20D, 200 South 6th Street, Minneapolis, MN 55402

|  |  |
| --- | --- |
| Equal Housing Lender | © 2021 U.S. Bank. Equal Housing Lender. Member FDIC. |

 |

 |

 |