

«Name»
«Street_Address»
«City», «State_mailing» «Zip_Code»

Notice of Data Security Incident

Dear «Name»,

We are contacting you because Quicken Inc. ("Quicken") recently experienced a data security incident related to our third-party customer care tracking system that could have included some of your personal information. Please review this letter carefully to learn about the incident and about the resources our company is providing to you to monitor your personal information and help protect yourself against identity theft.

What happened?

Quicken recently discovered that certain customer information collected as part of your conversation with our Customer Care team, and stored in Quicken's third-party customer relationship management system, was potentially vulnerable to unauthorized access. The vulnerability appears to have been present since 2019. **We have no evidence that any malicious actor actually accessed this information.** On or around February 1, 2021, Quicken became aware of the vulnerability, immediately corrected it, and identified certain personal information belonging to a small number of current and former Quicken customers that had potentially been at risk to unauthorized access. You are receiving this notice because you are one of a small group of people who Quicken determined may have had some of their personal information subject to the vulnerability.

Neither the Quicken software nor any Quicken-operated technology was affected by this incident.

What information was involved?

The personal information potentially vulnerable to access relates to information you provided during your conversation with Quicken's Customer Care representatives. In your case this included your Quicken data file which may contain financial institution information (but not passwords), email address, and phone number. **At this time, we do not have any evidence that the information was accessed by a malicious actor, misused in any way, nor that any individual has suffered from identity theft as a result of the incident.**

What are we doing?

Quicken takes this issue very seriously. After learning of the incident, we immediately corrected the vulnerability. We also modified our internal processes to further secure such data and our third-party systems.

Out of an abundance of caution, and as an added protection, Quicken is offering you a two-year membership to Equifax ID Patrol at no cost to you. This product provides you with superior detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- 1) Ensure that you enroll by: 6/30/21 (Your code will not work after this date.)
- 2) Visit the Equifax ID Patrol website to enroll: <http://www.myservices.equifax.com/patrol>
- 3) Provide your unique activation code: «Credit_monitoring_»

If you have questions about the product, or need assistance with activation, contact Equifax's Customer Care team at 1-866-640-2273 on or before June 30, 2021.

What you can do:

We recommend that you enroll in the Equifax program and, as always, remain vigilant for incidents of fraud and identity theft, including regularly viewing your account statements and monitoring your free credit reports. In addition, we recommend that you monitor your email for potential phishing attempts. For more information on how you can help protect yourself, please go to the page on our website which covers this topic in detail: www.quicken.com/phishing-prevention-tips.

For more information:

If you have any questions or concerns about this incident contact Quicken Care at 1-888-476-0041. We regret that this incident occurred and any inconvenience it may cause you. We thank you for your continued support.

Sincerely,



Pehr Lawson
VP Quicken Customer Care

Name
Address
City, State, Zip

Notice of Data Security Incident

Dear <first last>,

We are contacting you because Quicken Inc. ("Quicken") recently experienced a data security incident related to our third-party customer care tracking system that could have included some of your personal information. Please review this letter carefully to learn about the incident and about the resources our company is providing to you to monitor your personal information and help protect yourself against identity theft.

What happened?

Quicken recently discovered that certain customer information collected as part of your conversation with our Customer Care team, and stored in Quicken's third-party customer relationship management system, was potentially vulnerable to unauthorized access. The vulnerability appears to have been present since 2019. **We have no evidence that any malicious actor actually accessed this information.** On or around February 1, 2021, Quicken became aware of the vulnerability, immediately corrected it, and identified certain personal information belonging to a small number of current and former Quicken customers that had potentially been at risk to unauthorized access. You are receiving this notice because you are one of a small group of people who Quicken determined may have had some of their personal information subject to the vulnerability.

Neither the Quicken software, your Quicken data, nor any Quicken-operated technology was affected by this incident.

What information was involved?

The personal information potentially accessed relates to information you provided during your conversation with Quicken's Customer Care representatives. In your case this included your driver's license information, email address, and phone number. **At this time, we do not have any evidence that the information was accessed by a malicious actor, misused in any way, nor that any individual has suffered from identity theft as a result of the incident.**

What are we doing?

Quicken takes this issue very seriously. After learning of the incident, we immediately corrected the vulnerability. We also modified our internal processes to further secure such data and our third-party systems.

Out of an abundance of caution, and as an added protection, Quicken is offering you a two-year membership to Equifax ID Patrol at no cost to you. This product provides you with superior detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- 1) Ensure that you enroll by: 6/30/21 (Your code will not work after this date.)
- 2) Visit the Equifax ID Patrol website to enroll: <http://www.myservices.equifax.com/patrol>
- 3) Provide your unique activation code: [code]

If you have questions about the product, or need assistance with activation, contact Equifax's Customer Care team at 1-866-640-2273 on or before June 30, 2021.

What you can do:

We recommend that you enroll in the Equifax program and, as always, remain vigilant for incidents of fraud and identity theft, including regularly viewing your account statements and monitoring your free credit reports. In addition, we recommend that you monitor your email for potential phishing attempts. For more information on how you can help protect yourself, please go to the page on our website which covers this topic in detail: www.quicken.com/phishing-prevention-tips.

For more information:

If you have any questions or concerns about this incident contact Quicken Care at 1-888-476-0041. We regret that this incident occurred and any inconvenience it may cause you. We thank you for your continued support.

Sincerely,



Pehr Lawson
VP Quicken Customer Care