



DLA Piper LLP (US)
1201 North Market Street
Suite 2100
Wilmington, Delaware 19801-1147

Edward J. McAndrew
(302) 468-5685
Ed.McAndrew@us.dlapiper.com

June 2, 2022

VIA EMAIL: IDTHEFTX5@OAG.STATE.MD.US

The Honorable Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Security Incident Notification

Dear Attorney General Frosh:

We are providing notice on behalf of On Deck Capital, Inc. (“OnDeck”) pursuant to Md. Code Ann. Comm. Law § 14-3504, about an incident involving 1,169 Maryland residents.

On March 10, 2022, OnDeck’s security team detected suspicious activity on a limited number of internal computers, which were quickly taken offline. OnDeck notified the Federal Bureau of Investigation and immediately launched its own comprehensive investigation with the assistance of leading cybersecurity experts. On March 13, 2022, OnDeck learned that an unauthorized actor copied certain OnDeck data to a private cloud storage account.

On March 17, 2022, OnDeck’s investigators gained sole control over this private cloud storage account. OnDeck’s investigators recovered the data contained in the account and have informed OnDeck that the account is disabled. OnDeck’s investigation confirmed that the data was not otherwise accessed while stored in this account. Since recovering the data, OnDeck has worked with outside cybersecurity experts to analyze its contents, specifically with the aim of identifying any personal information contained in the data. On May 17, 2022, OnDeck determined that a limited amount of personal information of 1,169 Maryland residents was contained in the data set that OnDeck recovered from the private cloud storage account.

The types of personal information contained in the data set varied by individual, and not all types of information were present for each individual. In general, the data set included one or more of the following types of personal information: Name, Social Security Number, Tax ID Number, Driver’s License Number, Passport Number, financial account/payment card account number, and medical or health insurance information.

The monitoring and security systems OnDeck had in place enabled it to quickly identify and respond to the incident. Upon becoming aware of the incident, OnDeck promptly launched an investigation with the assistance of leading cybersecurity experts and took steps to determine the



The Honorable Brian E. Frosh
June 2, 2022
Page Two

nature and scope of any unauthorized access to OnDeck data. OnDeck has taken a number of security and remediation steps, including enhancing identity and access management controls, blocking suspicious Internet traffic, resetting account credentials, and deploying additional continuous monitoring solutions. OnDeck also have notified and continues to work with the FBI on its investigation of this incident.

In an abundance of caution, OnDeck is notifying potentially affected individuals and providing them with a complimentary 24-month membership of Experian's IdentityWorks, which includes credit monitoring, fraud consultation, and identity theft restoration.

OnDeck intends to mail notification letters to the affected Maryland residents on or about June 2, 2022. A sample of the notification letter is attached.

If you should have any questions or if we can provide further assistance to the Maryland residents affected by this incident, please feel free to contact me at (302) 468-5685 or ed.mcandrew@us.dlapiper.com.

Respectfully submitted,

DLA Piper LLP (US)

A handwritten signature in blue ink, appearing to read 'Ed McAndrew', with a long horizontal flourish extending to the right.

Edward J. McAndrew

Counsel for On Deck Capital, Inc.

Enclosure



1400 Broadway
New York, NY 10018

June 2, 2022



H9366-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



RE: Notice of Data [Extra1]

Dear Sample A. Sample:

We write to share important information with you about a data security incident that may have affected your personal information held by OnDeck. Out of an abundance of caution, we are providing you with this notice so that you know what we are doing and the steps you can take to protect your information should you feel it is appropriate to do so. We regret that this incident occurred and take the security of your information seriously.

What Happened?

On March 10, 2022, OnDeck's security team detected suspicious activity on a limited number of internal computers, which were quickly taken offline. OnDeck immediately launched its own comprehensive investigation with the assistance of leading cybersecurity experts and notified the Federal Bureau of Investigation of its investigation. On March 13, 2022, OnDeck learned that an unauthorized actor copied certain OnDeck data to a private cloud storage account.

On March 17, 2022, OnDeck's investigators gained sole control over this private cloud storage account. OnDeck's investigators recovered the data contained in the account and have informed OnDeck that the account is disabled. OnDeck's investigation confirmed that the data was not otherwise accessed while stored in this account. Since recovering the data, OnDeck has worked with outside cybersecurity experts to analyze its contents, specifically with the aim of identifying any personal information contained in the data. On May 17, 2022, OnDeck determined that a limited amount of personal information about you was contained in the data set that OnDeck recovered from the private cloud storage account.

What Information Was Involved?

The types of personal information contained in the data set varied by individual, and not all types of information were present for each individual. In general, the data set included one or more of the following types of personal information: Name, Social Security Number, Tax ID Number, Driver's License Number, Passport Number, financial account/payment card account number, and medical or health insurance information.

0000001



H9366-L01

What Are We Doing?

Protecting your personal information is of paramount importance to OnDeck. The monitoring and security systems we had in place enabled us to quickly identify and respond to the incident. Upon becoming aware of the incident, we promptly launched an investigation with the assistance of leading cybersecurity experts and took steps to determine the nature and scope of any unauthorized access to OnDeck data. We have taken a number of security and remediation steps, including enhancing identity and access management controls, blocking suspicious Internet traffic, resetting account credentials, and deploying additional continuous monitoring solutions. We also have notified and are working with law enforcement on its investigation of this incident.

As an added precaution, we have arranged to have Experian, a global leader in risk mitigation and response, provide identity monitoring at no cost to you for two years. As detailed below, your complimentary identity monitoring services include Credit Monitoring, Identity Theft Restoration, and Identity Theft Insurance.

What Can You Do?

There are important steps that you can take to reduce the potential risk of fraud and/or identity theft.

We are providing you with access to a complimentary 24-month membership of Experian's IdentityWorks. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: August 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 397-0031 by **August 31, 2022**. Be prepared to provide engagement number **B053847** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 397-0031. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for twenty-four (24) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

For More Information

We have included some additional information below regarding other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report.

If you have any further questions regarding this incident, please call the dedicated and confidential toll-free telephone line that we have set up to respond to questions, at (888) 397-0031. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9:00am to 9:00pm Pacific Time and Saturday & Sunday, 9:00am to 6:00pm Pacific Time.

I would like to reiterate that the security of your personal information is among our highest priorities. We sincerely regret any inconvenience caused to you by this incident.

Sincerely,



Jim Granat
Head of SMB Lending



Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

	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 Fraud Alert Form	https://www.experian.com/fraud/center.html	https://www.equifax.com/personal/credit-report-services/	https://fraud.transunion.com/fa/fraudAlert/landingPage.jsp

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised 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. Under federal law, you cannot be charged to place, lift or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

	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

To request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

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, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver’s license or ID card, military identification, etc.);

7. Social Security Card, pay stub, or W2;
8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission. This notice has not been delayed by law enforcement.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above.

District of Columbia Residents: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001
(202) 727-3400
<https://oag.dc.gov/>

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
Telephone: 1-888-743-0023.
www.oag.state.md.us/Consumer

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of



credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina
9001 Mail Service Center
Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
www.ncdoj.gov

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.