



July 26, 2017

**RECEIVED**

**JUL 27 2017**

**Orrick, Herrington & Sutcliffe LLP**

1000 Marsh Road  
Menlo Park, CA 94025-1015

+1 650 614 7400

orrick.com

Office of the Attorney General  
Consumer Protection and Antitrust Bureau  
33 Capitol Street  
Concord, NH 03301

**CONSUMER PROTECTION**

**Jacob M. Heath**

E jheath@orrick.com

D +1 650 614 7321

F +1 650 614 7401

Re: **Notice of Security Incident – New Hampshire**

To Whom It May Concern:

Please find the attached notice of data security incident.

Best regards,

Jacob M. Heath

Enclosure

July 26, 2017

Office of the Attorney General  
Consumer Protection and Antitrust Bureau  
33 Capitol Street  
Concord, NH 03301

VIA MAIL

Re: Notification of Information Security Incident

Dear Sir or Madam:

I write to inform you of a security incident experienced by Virgin America that involved the personal information of one (1) individual who is a resident of New Hampshire. Virgin America is an airline with its headquarters located at 555 Airport Boulevard, Suite 400, Burlingame, CA 94010.

On March 13, 2017, during security monitoring activities, our data security team identified potential unauthorized access to Virgin America computer systems. Our investigation determined that an unauthorized third party may have had access to personal information of certain Virgin America employees and contractors. The affected personal information includes login and password information used to gain access to Virgin America's corporate network, as well as other personal information which could potentially include a full name, address, Social Security number, driver's license or government issued ID or health information. No customer or cardholder data was affected.

Safeguarding personal information is important to Virgin America. We immediately initiated our incident response plan, engaged cybersecurity experts to investigate, and notified law enforcement. We also began immediately remediating affected Virgin America systems, which included telling all Virgin America employees and contractors to reset their passwords. We also initiated a review of our security procedures and protocols, and we have already implemented changes to reduce the possibility of this happening again.

Virgin America will send written notification letters to affected individuals this week by mail in substantially the same form as the attached sample. Although we have no reason to believe that any individual's information was misused, as a precaution, we are offering one year of credit monitoring and identity theft protection services provided by Kroll, at no cost to the affected individuals.

Please do not hesitate to contact me at [kyle.levine@alaskaair.com](mailto:kyle.levine@alaskaair.com) or by phone at 206.392.5292.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'K. Levine', with a long horizontal stroke extending to the right.

Kyle Levine

Vice President, Legal and General Counsel  
Alaska Air Group, Inc.

Attachment



<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<ZipCode>>

**Re: Notice of Data Breach of Virgin America Systems**

Dear <<MemberFirstName>> <<MemberLastName>>,

Today, I am writing on behalf of Virgin America's information technology and information security teams to notify you that an outside party gained unauthorized access to certain Virgin America information systems containing your data. In this letter, you'll find the steps our data security team have taken and information about the resources we are offering to help you protect yourself.

**What Happened?**

On March 13, 2017, during security monitoring activities, our data security team identified potential unauthorized access to certain Virgin America computer systems. We immediately took steps to respond to the incident, including initiating our incident response protocol and taking measures to mitigate the impact to affected individuals. We retained cybersecurity forensic experts to investigate the incident and reported the matter to law enforcement. Nevertheless, it appears that a third party may have accessed information about certain Virgin America employees and contractors without authorization.

**What Information Was Involved**

The unauthorized third party gained access to your login information and password that you use to access Virgin America's corporate network; as well as personal information, potentially including your name, address, Social Security number, driver's license or government issued ID, or health-related information.

**What We Are Doing**

We do not have evidence that your personal information was misused in any way. As a precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

*You have until <<Date>> to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-???-???-?????. Additional information describing your services is included with this letter.

**What You Can Do**

We encourage you to contact Kroll and activate the services provided to you. It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review your bank and credit card statement and credit reports for any unauthorized activity. Report suspected incidents of fraud or identity theft promptly. You should also regularly

rotate your password for your online accounts and not use the same password for multiple accounts. We have enclosed a Resources Guide containing contact information for the three national consumer reporting agencies and other information which you may find helpful.

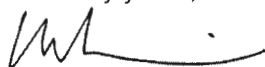
If you suspect that you are a victim of identity theft or fraud, you have the right to file a police report and obtain a copy of it. In addition, you may contact your State Attorney General's office or the Federal Trade Commission to learn about the steps you can take to protect yourself against identify theft. We have summarized this information for you in the Resources Guide, enclosed with this letter.

You should also be alert to email "phishing" attacks by someone who acts like a colleague or friend and requests sensitive information over email, such as passwords, Social Security numbers, or bank account numbers.

#### **For More Information**

I understand that this may come as a surprise. I want to assure you that our information security teams are working hard to enhance our privacy and security practices here at Virgin America to reduce the likelihood that something like this happens again. If you have any additional questions about the information contained in this letter, please contact Kroll at 1-800-870-8700 8 a.m. – 5 p.m. CT, Monday through Friday, excluding major holidays.

Sincerely yours,



Kyle Levine, Vice President, Legal and General Counsel  
Alaska Air Group, Inc.

## IDENTITY THEFT RESOURCES GUIDE - UNITED STATES

**U.S. Federal Trade Commission (FTC):** The FTC has information about how to avoid identity theft and other steps that consumers can take to protect themselves. Write to: Consumer Response Center, 600 Pennsylvania Ave., NW, H-130, Washington, D.C. 20580; Call Toll-Free: 1-877-IDTHEFT (438-4338); or Visit: <http://www.ftc.gov/idtheft>

**For IOWA Residents:** You may contact local law enforcement or the Iowa Attorney General's Office at 1305 E. Walnut St., Des Moines, IA 50319; Tel: (515) 281-5164; or <http://www.iowa.gov/government/ag>

**For MARYLAND Residents:** You may obtain information about preventing identity theft from the FTC or the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202; Tel: (888) 743-0023; or <http://www.oag.state.md.us>

**For NORTH CAROLINA Residents:** You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699-9001; Tel: (919) 716-6400; Fax: (919) 716-6750; or <http://www.ncdoj.com>

**For RHODE ISLAND Residents:** You may obtain information about preventing identity theft from the FTC or the Rhode Island Attorney General's Office at 150 South Main Street, Providence, RI 02903; Tel: (401) 274-4400; or <http://www.riag.ri.gov>

**Free Annual Credit Report:** You may obtain a free copy of your credit report once every 12 months and may purchase additional copies of your credit report. Call Toll-Free: 1-877-322-8228; or Visit: <https://www.annualcreditreport.com>; or Contact any one or more of the consumer reporting agencies:

Equifax:	P.O. Box 740241, Atlanta, GA 30374-0241	(800) 685-1111	<a href="http://www.equifax.com">www.equifax.com</a>
Experian:	P.O. Box 2002, Allen, TX 75013	(888) 397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion:	P. O. Box 1000, Chester, PA 19022	(800) 888-4213	<a href="http://www.transunion.com">www.transunion.com</a>

### **"Fraud Alerts" and "Security Freezes"**

**Fraud Alert:** You may have the right to place a fraud alert in your file to alert potential creditors that you may be a victim of identity theft. Creditors must then follow certain procedures to protect you; therefore, a fraud alert may delay your ability to obtain credit. An "initial fraud alert" stays in your file for at least 90 days. An "extended fraud alert" stays in your file for 7 years, and will require an identity theft report (usually, a filed police report). You may place a fraud alert by calling any one of the three national consumer reporting agencies:

Equifax: 1-800-525-6285                      Experian: 1-888-397-3742                      TransUnion: 1-800-680-7289

**Security Freeze:** Certain U.S. state laws, including in Massachusetts, provide the right to place a security freeze on your credit file, which prevents credit, loans and services from being approved in your name without your consent. Using a freeze may interfere with or delay your ability to obtain credit. To place a freeze, send a request by mail to each consumer reporting agency (addresses below) with the following (if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) Full name, with middle initial and any suffixes; (2) Social Security Number; (3) Date of Birth; (4) proof of current address (such as a utility bill or telephone bill) and list of any previous addresses for the past five years; (5) copy of a government issued identity card, and (6) copy of police report, investigative report or complaint to law enforcement regarding identity theft. The consumer reporting agency may charge a fee up to \$5.00 to place, lift, and/or remove a freeze, unless you are a victim of identity theft or the spouse of a victim, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. The consumer reporting agencies have three business days after receiving your letter to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN or password that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the consumer reporting agencies by mail and include proper identification (name, address, and SSN) 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 or the specific period of time you want the credit report available. The consumer reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and SSN) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the freeze.

Equifax Security Freeze: P.O. Box 105788, Atlanta, Georgia 30348

Experian Security Freeze: P.O. Box 9554, Allen, TX 75013

TransUnion (Fraud Victim Assistance Division): P.O. Box 6790, Fullerton, CA 92834-6790



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

### **Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### **Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

### **Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### **\$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.