



Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Kamran.Salour@lewisbrisbois.com
Direct: 714.966.3145

September 10, 2021

File No. 30841.1602

INTENDED FOR ADDRESSEE(S) ONLY

VIA E-MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

Lewis Brisbois Bisgaard & Smith LLP represents In-Flight Crew Connections, Inc. (“IFCC”) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire’s data breach notification statute.

1. Nature of the Security Incident

IFCC is a staffing agency located in Charlotte, North Carolina.

On March 25, 2021, IFCC learned of unusual activity within its email environment. Upon discovering this incident, IFCC took immediate steps to secure the environment. IFCC also launched an investigation and engaged a digital forensics firm to determine what happened and what information may have been accessed.

The investigation revealed that an unauthorized actor was able to access three IFCC email accounts. Based on the findings from the investigation, IFCC reviewed the affected account to determine what data might have been impacted and determined that the impacted account contained some of your personal information. IFCC then worked diligently to identify addresses for the individuals whose information may have been involved. IFCC completed that process on August 17, 2021.

2. Type of Information and Number of New Hampshire Residents Involved

The incident involved personal information for approximately 1 New Hampshire resident. The information involved varies for each individual, but may include Social Security information and passport number.

The affected individual will receive a letter notifying them of the incident, offering complimentary identity monitoring services, and providing additional steps they can take to protect their personal information. The notification letters will be sent via USPS First Class Mail on September 10, 2021.

3. Measures Taken to Address the Incident

In response to the incident, IFCC retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise.

Additionally, as discussed above, IFCC is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

IFCC is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Kamran Salour at 714.966.3145 or Kamran.Salour@lewisbrisbois.com.

Sincerely,



Kamran Salour of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

KS:vhv
Encl.: Sample Notification Letter



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Re: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We write to inform you of a data security incident that involved some of your personal information. At In-Flight Crew Connections, Inc. (“IFCC”) we take the privacy and security of our information very seriously. This is why we are notifying you of the incident, offering you identity monitoring services, and informing you about steps you can take to help protect your information.

What Happened: On March 25, 2021, IFCC learned of unusual activity within its email environment. Upon discovering this incident, IFCC took immediate steps to secure the environment. IFCC also launched an investigation and engaged a digital forensics firm to determine what happened and what information may have been accessed.

The investigation revealed that an unauthorized actor was able to access three IFCC email accounts. Based on the findings from the investigation, IFCC reviewed the affected account to determine what data might have been impacted and determined that the impacted account contained some of your personal information. IFCC then worked diligently to identify addresses for the individuals whose information may have been involved. IFCC completed that process on August 17, 2021. Importantly, IFCC is not aware of any misuse of your personal information as a result of this incident.

What Information Was Involved: The information may have involved your <<b2b_text_1(Name, Impacted Data)>>.

What Are We Doing: As soon as we discovered the incident, we took the steps described above. In addition, we are offering you with information about steps you can take to help protect your personal information, including free identity monitoring services for 12 months through Kroll as described below.

What You Can Do: You can follow the recommendations included with this letter to help protect your personal information. We strongly encourage you to activate the identity monitoring services we are offering through Kroll, a global leader in risk mitigation and response. Your services will include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Steps for activating your identity monitoring services are below:

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **December 12, 2021** to activate your identity monitoring services.*

Membership Number: <<Membership Number s_n>>

For More Information: If you have any questions about this letter, please call 1-??-??-?? from 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink that reads "Bryan Smith". The signature is written in a cursive style with a large initial "B".

Bryan Smith, Controller
In-Flight Crew Connections, Inc.

Steps You Can Take to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will be able to help you determine if it is 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 will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.