



February 10, 2009

Attorney General William H. Sorrell  
109 State St.  
Montpelier, VT 05609-1001

Dear Attorney General Sorrell:

We are writing to officially notify you of a possible breach of security of personal information involving approximately 1 Vermont residents.

#### **NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS**

On February 2/3, 2009 between the hours of 7:30 pm and 5:45 am a laptop computer was stolen from the accounting area at our facility located at 97 Libbey Parkway, Weymouth, MA, 02189. The laptop and data was password protected however the data was not encrypted. The data contained on this laptop included personal information for some of our active and non-active employees, shareholders, investors and aircraft owners. This laptop was assigned to a member of our Accounting Department who is responsible for tax related data. We are trying to ascertain the exact data that was stored on the hard drive at this time.

During the initial phase of our investigation we have been able to determine that the data maintained on the hard drive may have contained the following information for the time period 2004 - 2009:

1. Employee names,
2. Employee addresses,
3. Employee social security numbers or the last four digits of their social security numbers,
4. Employee bank routing and account numbers,
5. Shareholder/Investor names,
6. Shareholder/Investor addresses,
7. Shareholder/Investor social security numbers
8. K1 reports
9. Aircraft Owner identification to include names, addresses, and property tax information, and
10. Shareholder transactions.

#### **NUMBER OF VERMONT RESIDENTS AFFECTED**

At this time we are estimating that approximately 1 Vermont residents may have been affected along with approximately 2,226 other active/non-active employees located in AL, AZ, CA, CO, CT, DC, DE, FL, GA, HI, ID, IL, IN, KS, KY, LA, MA, MD, ME, MI, MN, MO, MS, MT, NC, NE, NH, NJ, NV, NY, OH, OK, OR, PA, RI, SC, SD, SK, TN, TX, UT, VA, VI, WA, WI and WV.

In accordance with the applicable regulatory requirements, we are in the process of preparing an electronic notification that will go out to all active employees (1,576, 1 of whom are Vermont residents) and written notification that will go out to all non-active employees (651, 0 of whom are Vermont residents). A copy of this letter will also be posted on our company intranet along with a copy of the Federal Trade Commission document titled "Take Charge: Fighting Back Against Identity Theft".



We are expecting to release the employee letter on Monday, February 9, 2009 to ensure that all active employees are notified at the same time. We will begin mailing out the written letters to non-active employees on Monday February 9, 2009 and anticipate completing the process by Wednesday, February 11, 2009. We understand the time sensitivity and are pulling in all of our resources to ensure the information is forwarded to all Vermont residents who may have been affected by the breach of security. A copy of the proposed employee letter is attached.

#### **STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT**

Upon notification of the incident, we immediately contacted the local law enforcement agency. A thorough investigation is in progress; they have interviewed several members of our team and are continuing to gather information. The District Attorney's Office as well as the Federal Bureau of Investigation (FBI) has been notified as well.

Our IT Department was contacted to re-release our company requirements on the retention of data on laptops, password protection procedures, equipment security, and the procedures for storing sensitive personal information. All active employees were forwarded this information on February 3, 2009.

The Director of Security conducted an audit of all employee identification badges and cleaning employees, ran reports on all facility access activity for the time period between February 2 and 3, 2009, reviewed access requirements with each employee, including the outsourced cleaners and re-activated the identification and access badges.

At this time JetDirect Holdings, LLC has no reason to believe that any personal information has been or will be accessed or misused.

Since the incident we have been conducting random checks of all office areas to verify that laptop and desktop equipment is secure. Checks have been accomplished at various times through the day and evenings to ensure that the procedures contained in the e-mail from our IT Department are being followed.

The letter we are forwarding to all employees, shareholders, investors and aircraft owners includes the names and telephone numbers for all three of the credit reporting agencies. We have recommended that they contact one of the agencies to place credit monitoring on their accounts and advised them that this free for a period of 90 days at which time they can renew the alert. We have also advised them to contact their local banking institution to discuss options available to them to protect their existing accounts.

#### **OTHER NOTIFICATION AND CONTACT INFORMATION**

A verbal notification was made to the Director of Consumer Affairs and Business Regulation on February 5, 2009. A copy of this package will be forwarded to them today to satisfy the official notification requirements.

Please feel free to contact Sheryle Milligan, Vice President of Safety, Security and Regulatory Compliance, JetDirect Aviation Holdings, LLC, 97 Libbey Parkway, Weymouth, MA 02189, Direct line 781.927.8215, Mobile 781.901.9939 or e-mail [smilligan@jetdirectaviation.com](mailto:smilligan@jetdirectaviation.com) if you have any questions or should you need any additional information.

Sincerely,

JetDirect Aviation Holdings, LLC

Sheryle A. Milligan  
Vice President of Safety, Security and Regulatory Compliance



February 9, 2009

Dear Former Employee:

We are writing to inform you of the theft of a laptop computer which may have contained certain personal information of JetDirect Aviation Holdings, LLC and its employees, as well as employees of each of its subsidiaries. There is currently no evidence to suggest that any of the information on the laptop has been misused. JetDirect is working closely with law enforcement authorities and is conducting its own investigation. We believe the theft occurred sometime between February 2, 2009 and February 3, 2009, from one of our corporate locations.

A complete description of the specific information contained on the laptop is unknown at this time, however we believe that, in addition to employee names, it may have included SOME employee social security numbers and/or employee bank account information that was used for payroll purposes. Steps are being taken to help ensure this type of incident does not happen again.

Because your social security number MAY HAVE been involved, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. Just call one of the three credit reporting agencies below. This will automatically place an alert with all of the agencies. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

Experian 1-888-397-3742

Equifax 1-800-525-6285

TransUnion 1-800-680-7289

When you receive your credit reports, look them over carefully, look for accounts you did not open, look for inquiries from creditors that you did not initiate, and look for personal information such as home address and social security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. You also should file a complaint with the FTC at 1-877-ID-THEFT (877-438-4338) or [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). Your complaint will be added to the FTC's Identify Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information is often held for use at different times. Checking your credit reports periodically can help you spot problems and address them quickly. You can keep the fraud alert in place by calling again after 90 days.

Additionally, because your bank account information MAY HAVE been involved, we recommend that you immediately contact your bank and tell them that your account may have been compromised, and discuss your options with them, including closing the account and opening a new account.

Again, we regret any inconvenience this may cause you, and will continue to pursue this matter.

Sincerely,

JetDirect Aviation Holdings, LLC

A handwritten signature in black ink that reads 'Sheryle A. Milligan'.

Sheryle A. Milligan  
Vice President Safety, Security & Regulatory Compliance



February 9, 2009

Dear Employee:

We are writing to inform you of the theft of a laptop computer which may have contained certain personal information of JetDirect Aviation Holdings, LLC and its employees, as well as employees of each of its subsidiaries. There is currently no evidence to suggest that any of the information on the laptop has been misused. JetDirect is working closely with law enforcement authorities and is conducting its own investigation. We believe the theft occurred sometime between February 2, 2009 and February 3, 2009, from one of our corporate locations.

A complete description of the specific information contained on the laptop is unknown at this time, however we believe that, in addition to employee names, it may have included SOME employee social security numbers and/or employee bank account information that was used for payroll purposes. Steps are being taken to help ensure this type of incident does not happen again.

Because your social security number MAY HAVE been involved, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as "reasonable policies and procedures" to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. Just call one of the three credit reporting agencies at the number below. This will let you automatically place an alert with all of the agencies. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

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

When you receive your credit reports, look them over carefully, look for accounts you did not open, look for inquiries from creditors that you did not initiate, and look for personal information such as home address and social security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. You also should file a complaint with the FTC at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identify Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly. You can keep the fraud alert in place by calling again after 90 days.

Additionally, because your bank account information MAY HAVE been involved, we recommend that you immediately contact your bank and tell them that your account may have been compromised, and discuss your options with them, including closing the account and opening a new account.

In an attempt to provide you with as much information as possible we have uploaded a copy of the FTC document "Take Charge: Fighting Back Against Identify Theft" which is a comprehensive guide from the FTC to help you guard against and deal with identity theft on to the BAP Portal, Shared Documents. You can access this document by clicking on the link below.

<https://bap.jetdirectaviation.com/safc/Shared%20Documents/Forms/AllItems.aspx>

Again, we regret any inconvenience this may cause you, and will continue to pursue this matter.

Sincerely,

JetDirect Aviation Holdings, LLC

Sheryle A. Milligan  
Vice President Safety, Security & Regulatory Compliance