



D.A. Davidson & Co.  
Davidson Trust Co.  
Davidson Investment Advisors  
Davidson Travel

CONFIDENTIAL

February 4, 2008

Office of the Attorney General  
One Ashburton Place  
Boston, MA 02108

Re: Security Breach Notification

Dear State Official:


D.A. Davidson & Co. is a licensed broker-dealer in your state. This is to inform your Department that D.A. Davidson & Co. commenced mailing notices on January 29, 2008 to approximately 450 current and former clients residing in your state that a company database was illegally accessed by a third party through a sophisticated network intrusion. We have notified law enforcement and our principal regulatory authorities, including the agency responsible for securities regulation in your state, and are closely monitoring and assisting with the investigation. We have also notified the three principal credit reporting bureaus.

Attached is the form of notice sent to affected customers, which includes information on what actions consumers may take to protect themselves from fraud and identity theft, how to request that fraud alerts be placed on their individual credit files, and offers to provide to them, at our expense, a one-year enrollment to a three-bureau credit monitoring service, if they choose to access it.

The incident affected some customers residing in every state; however, the large majority of the affected customers reside in the western states, notably, Montana, Oregon, Washington, Idaho, and Wyoming.

Please contact me directly at 406-268-3056 if you have any questions.

Sincerely,

  
Larry Martinez  
SVP and General Counsel



January 29, 2008

### **Important Notice Regarding Your Personal Information**

Dear Valued Client:

D.A. Davidson is writing to inform you that a company database which contained confidential information about our current and former clients was illegally accessed by a third party through a sophisticated network intrusion. The information accessed may have included your name, address, email address, account number, Social Security or tax identification number, date of birth, November account balance, and your financial consultant's ID number. We have notified law enforcement and our regulatory authorities and are closely monitoring and assisting with the investigation.

The accessed database did not include other account information or detail and we do not believe the unauthorized access enabled the third party to effect or alter your accounts through our systems.

We are concerned about the possible misuse of your personal information, and we are writing so that you may take steps to protect yourself from fraud and identity theft. In light of the intrusion, we encourage you to review your D.A. Davidson account for any unauthorized activity, and if you have questions please contact your financial consultant directly (your financial consultant's phone number is on your statement) or the toll-free number provided below so we can assist you.

Because the intruder may have accessed your Social Security number, we recommend that you contact your credit and bank card issuers to review your most recent card charges and bank account transactions. If you discover that unauthorized charges appear on your accounts, please contact your card issuers right away to request that your current account be closed and a new card be issued.

As a further precaution, you may wish to place a fraud alert on your credit file. Specific information about protecting your credit lines and financial information is enclosed with this letter. *Please review it closely.* We also recommend that you review the identity theft materials posted for consumers on the Federal Trade Commission's (the "FTC's") Web site, [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/), and in particular, the posted copy of the FTC's booklet, *"Take Charge: Fighting Back Against Identity Theft."*

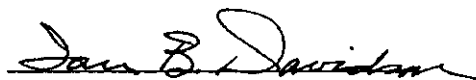
We endeavor to provide our clients with the highest levels of client service. To this end, we are reaching out to support those clients who may have been affected by this unfortunate incident:

- Should you have any questions about this incident or need additional information, you may contact your financial consultant directly, or, if they are not available, we have set up a special number for you to call, **1-800-909-6485.**
- We would like to offer you, at our expense, a one-year enrollment to Experian's Triple Advantage<sup>SM</sup> three-bureau credit monitoring product to help you begin the process of regularly reviewing your account records for any abnormalities. If you choose to enroll in the membership, please contact us at the toll-free number above and our representatives will help enroll you.

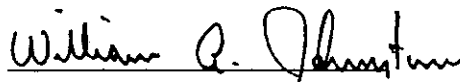
We also have contacted the three principal credit reporting bureaus, Equifax, Experian and TransUnion, to advise them of the situation. In addition, we have adopted measures to further enhance our network security and have deployed additional account monitoring procedures directed at detecting unauthorized activity on client accounts.

We regret the occurrence of this incident and any inconvenience it may have caused you. We value our relationship with you and want to work through this matter with you. If you have further questions, please do not hesitate to call your financial consultant or the toll-free number referred to above.

Sincerely,



Ian B. Davidson  
Chairman



William A. Johnstone  
President and CEO

### Steps to take to protect your credit and identity

Should you ever believe your identity has been stolen or that you are at risk of having your identity stolen, you can follow the Federal Trade Commission's ("FTC's") guidelines on protecting yourself against identity theft. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them.

First, you should contact your credit and bank card issuers as soon as possible to review your accounts for unauthorized charges or transactions. If there are unauthorized charges or if you otherwise believe that your card number has been taken by an unauthorized person, you should inform your card issuer on the phone and in writing that the charges were not authorized by you, and you should request that your current card account be closed and a new card issued in your name.

You may wish to consider placing a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing credit accounts. Because creditors seek additional verification from you when a fraud alert is in place on your credit file, one effect of the fraud alert is that it slows the processing time for opening new accounts and making changes on your existing accounts.

To place a fraud alert on your credit file, call any one of the three major credit bureaus. As soon as one credit bureau processes your fraud alert, it will notify the other credit bureaus on your behalf to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax  
1-800-525-6285

Experian  
1-888-397-3742

TransUnionCorp  
1-800-680-7289

You may also have right under applicable state law to request a "security freeze" on your credit report. A security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization.

Even if you do not initially find any suspicious activity on your card accounts, credit reports and/or bank statements, the FTC recommends that you check your credit reports, card charges and financial statements regularly. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports, card charges and financial statements periodically can help you spot problems and address them quickly. Once a year you can obtain a free credit report by calling 1-877-322-8228 or going online to [www.annualcreditreport.com](http://www.annualcreditreport.com).

If you find suspicious activity on your accounts or have reason to believe that your personal information is being misused, it may be necessary for you to file a police report and obtain a copy of that police report. Many creditors require the information the police report contains to absolve you of the fraudulent debts.

You may also want to file a complaint with the FTC, which will be logged into its database of identity theft cases used by law enforcement agencies for investigations. To get free information or file a complaint with the FTC, you may call the FTC at 1-877-438-4338, or use the complaint form at <http://www.consumer.gov/idtheft/>.



[REDACTED]  
[REDACTED]  
[REDACTED]

January 29, 2008

### **Important Notice Regarding Your Personal Information**

Dear Former Client:

D.A. Davidson is writing to inform you that a company database which contained confidential information about our current and former clients was illegally accessed by a third party through a sophisticated network intrusion. The information accessed may have included your name, address and email address last on record with us, Social Security or tax identification number, and date of birth. We have notified law enforcement and our regulatory authorities and are closely monitoring and assisting with the investigation.

We are concerned about the possible misuse of your personal information, and we are writing so that you may take steps to protect yourself from fraud and identity theft. Because the intruder may have accessed your Social Security number, we recommend that you contact your credit and bank card issuers to review your most recent card charges and bank account transactions. If you discover that unauthorized charges appear on your accounts, please contact your card issuers right away to request that your current account be closed and a new card be issued.

As a further precaution, you may wish to place a fraud alert on your credit file. Specific information about protecting your credit lines and financial information is enclosed with this letter. *Please review it closely.* We also recommend that you review the identity theft materials posted for consumers on the Federal Trade Commission's (the "FTC's") Web site, [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/), and in particular, the posted copy of the FTC's booklet, *"Take Charge: Fighting Back Against Identity Theft."*

We are reaching out to assist those former clients who may have been affected by this unfortunate incident:

- Should you have any questions about this incident or need additional information, please contact us at the special number we have set up for you, **1-800-736-6153**.
- We would like to offer you, at our expense, a one-year enrollment to Experian's Triple Advantage<sup>SM</sup> three-bureau credit monitoring product to help you begin the process of regularly reviewing your account records for any abnormalities. If you choose to enroll in the membership, please contact us at the toll-free number above and our representatives will help enroll you.

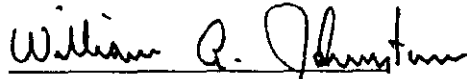
We also have contacted the three principal credit reporting bureaus, Equifax, Experian and TransUnion, to advise them of the situation.

We regret the occurrence of this incident and any inconvenience it may have caused you. If you have further questions or concerns, please do not hesitate to call the toll-free number referred to above.

Sincerely,



Ian B. Davidson  
Chairman



William A. Johnstone  
President and CEO

### Steps to take to protect your credit and identity

Should you ever believe your identity has been stolen or that you are at risk of having your identity stolen, you can follow the Federal Trade Commission's ("FTC's") guidelines on protecting yourself against identity theft. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them.

First, you should contact your credit and bank card issuers as soon as possible to review your accounts for unauthorized charges or transactions. If there are unauthorized charges or if you otherwise believe that your card number has been taken by an unauthorized person, you should inform your card issuer on the phone and in writing that the charges were not authorized by you, and you should request that your current card account be closed and a new card issued in your name.

You may wish to consider placing a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing credit accounts. Because creditors seek additional verification from you when a fraud alert is in place on your credit file, one effect of the fraud alert is that it slows the processing time for opening new accounts and making changes on your existing accounts.

To place a fraud alert on your credit file, call any one of the three major credit bureaus. As soon as one credit bureau processes your fraud alert, it will notify the other credit bureaus on your behalf to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax  
1-800-525-6285

Experian  
1-888-397-3742

TransUnionCorp  
1-800-680-7289

You may also have right under applicable state law to request a "security freeze" on your credit report. A security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization.

Even if you do not initially find any suspicious activity on your card accounts, credit reports and/or bank statements, the FTC recommends that you check your credit reports, card charges and financial statements regularly. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports, card charges and financial statements periodically can help you spot problems and address them quickly. Once a year you can obtain a free credit report by calling 1-877-322-8228 or going online to [www.annualcreditreport.com](http://www.annualcreditreport.com).

If you find suspicious activity on your accounts or have reason to believe that your personal information is being misused, it may be necessary for you to file a police report and obtain a copy of that police report. Many creditors require the information the police report contains to absolve you of the fraudulent debts.

You may also want to file a complaint with the FTC, which will be logged into its database of identity theft cases used by law enforcement agencies for investigations. To get free information or file a complaint with the FTC, you may call the FTC at 1-877-438-4338, or use the complaint form at <http://www.consumer.gov/idtheft/>.



D.A. Davidson & Co.  
Davidson Trust Co.  
Davidson Investment Advisors  
Davidson Travel

CONFIDENTIAL

February 4, 2008

Office of the Attorney General  
One Ashburton Place  
Boston, MA 02108

Re: Security Breach Notification

Dear State Official:


D.A. Davidson & Co. is a licensed broker-dealer in your state. This is to inform your Department that D.A. Davidson & Co. commenced mailing notices on January 29, 2008 to approximately 450 current and former clients residing in your state that a company database was illegally accessed by a third party through a sophisticated network intrusion. We have notified law enforcement and our principal regulatory authorities, including the agency responsible for securities regulation in your state, and are closely monitoring and assisting with the investigation. We have also notified the three principal credit reporting bureaus.

Attached is the form of notice sent to affected customers, which includes information on what actions consumers may take to protect themselves from fraud and identity theft, how to request that fraud alerts be placed on their individual credit files, and offers to provide to them, at our expense, a one-year enrollment to a three-bureau credit monitoring service, if they choose to access it.

The incident affected some customers residing in every state; however, the large majority of the affected customers reside in the western states, notably, Montana, Oregon, Washington, Idaho, and Wyoming.

Please contact me directly at 406-268-3056 if you have any questions.

Sincerely,

  
Larry Martinez  
SVP and General Counsel



[REDACTED] Inc.  
[REDACTED]  
[REDACTED]

January 29, 2008

**Important Notice Regarding Your Personal Information**

Dear Valued Client:

D.A. Davidson is writing to inform you that a company database which contained confidential information about our current and former clients was illegally accessed by a third party through a sophisticated network intrusion. The information accessed may have included your name, address, email address, account number, Social Security or tax identification number, date of birth, November account balance, and your financial consultant's ID number. We have notified law enforcement and our regulatory authorities and are closely monitoring and assisting with the investigation.

The accessed database did not include other account information or detail and we do not believe the unauthorized access enabled the third party to effect or alter your accounts through our systems.

We are concerned about the possible misuse of your personal information, and we are writing so that you may take steps to protect yourself from fraud and identity theft. In light of the intrusion, we encourage you to review your D.A. Davidson account for any unauthorized activity, and if you have questions please contact your financial consultant directly (your financial consultant's phone number is on your statement) or the toll-free number provided below so we can assist you.

Because the intruder may have accessed your Social Security number, we recommend that you contact your credit and bank card issuers to review your most recent card charges and bank account transactions. If you discover that unauthorized charges appear on your accounts, please contact your card issuers right away to request that your current account be closed and a new card be issued.

As a further precaution, you may wish to place a fraud alert on your credit file. Specific information about protecting your credit lines and financial information is enclosed with this letter. *Please review it closely.* We also recommend that you review the identity theft materials posted for consumers on the Federal Trade Commission's (the "FTC's") Web site, [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/), and in particular, the posted copy of the FTC's booklet, *"Take Charge: Fighting Back Against Identity Theft."*

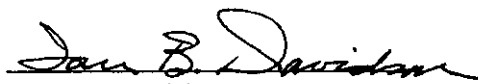
We endeavor to provide our clients with the highest levels of client service. To this end, we are reaching out to support those clients who may have been affected by this unfortunate incident:

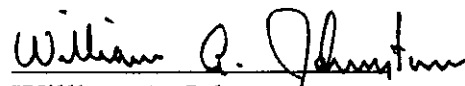
- Should you have any questions about this incident or need additional information, you may contact your financial consultant directly, or, if they are not available, we have set up a special number for you to call, **1-800-909-6485.**
- We would like to offer you, at our expense, a one-year enrollment to Experian's Triple Advantage<sup>SM</sup> three-bureau credit monitoring product to help you begin the process of regularly reviewing your account records for any abnormalities. If you choose to enroll in the membership, please contact us at the toll-free number above and our representatives will help enroll you.

We also have contacted the three principal credit reporting bureaus, Equifax, Experian and TransUnion, to advise them of the situation. In addition, we have adopted measures to further enhance our network security and have deployed additional account monitoring procedures directed at detecting unauthorized activity on client accounts.

We regret the occurrence of this incident and any inconvenience it may have caused you. We value our relationship with you and want to work through this matter with you. If you have further questions, please do not hesitate to call your financial consultant or the toll-free number referred to above.

Sincerely,

  
Ian B. Davidson  
Chairman

  
William A. Johnstone  
President and CEO

### Steps to take to protect your credit and identity

Should you ever believe your identity has been stolen or that you are at risk of having your identity stolen, you can follow the Federal Trade Commission's ("FTC's") guidelines on protecting yourself against identity theft. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them.

First, you should contact your credit and bank card issuers as soon as possible to review your accounts for unauthorized charges or transactions. If there are unauthorized charges or if you otherwise believe that your card number has been taken by an unauthorized person, you should inform your card issuer on the phone and in writing that the charges were not authorized by you, and you should request that your current card account be closed and a new card issued in your name.

You may wish to consider placing a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing credit accounts. Because creditors seek additional verification from you when a fraud alert is in place on your credit file, one effect of the fraud alert is that it slows the processing time for opening new accounts and making changes on your existing accounts.

To place a fraud alert on your credit file, call any one of the three major credit bureaus. As soon as one credit bureau processes your fraud alert, it will notify the other credit bureaus on your behalf to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax  
1-800-525-6285

Experian  
1-888-397-3742

TransUnionCorp  
1-800-680-7289

You may also have right under applicable state law to request a "security freeze" on your credit report. A security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization.

Even if you do not initially find any suspicious activity on your card accounts, credit reports and/or bank statements, the FTC recommends that you check your credit reports, card charges and financial statements regularly. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports, card charges and financial statements periodically can help you spot problems and address them quickly. Once a year you can obtain a free credit report by calling 1-877-322-8228 or going online to [www.annualcreditreport.com](http://www.annualcreditreport.com).

If you find suspicious activity on your accounts or have reason to believe that your personal information is being misused, it may be necessary for you to file a police report and obtain a copy of that police report. Many creditors require the information the police report contains to absolve you of the fraudulent debts.

You may also want to file a complaint with the FTC, which will be logged into its database of identity theft cases used by law enforcement agencies for investigations. To get free information or file a complaint with the FTC, you may call the FTC at 1-877-438-4338, or use the complaint form at <http://www.consumer.gov/idtheft/>.



January 29, 2008

### Important Notice Regarding Your Personal Information

Dear Former Client:

D.A. Davidson is writing to inform you that a company database which contained confidential information about our current and former clients was illegally accessed by a third party through a sophisticated network intrusion. The information accessed may have included your name, address and email address last on record with us, Social Security or tax identification number, and date of birth. We have notified law enforcement and our regulatory authorities and are closely monitoring and assisting with the investigation.

We are concerned about the possible misuse of your personal information, and we are writing so that you may take steps to protect yourself from fraud and identity theft. Because the intruder may have accessed your Social Security number, we recommend that you contact your credit and bank card issuers to review your most recent card charges and bank account transactions. If you discover that unauthorized charges appear on your accounts, please contact your card issuers right away to request that your current account be closed and a new card be issued.

As a further precaution, you may wish to place a fraud alert on your credit file. Specific information about protecting your credit lines and financial information is enclosed with this letter. *Please review it closely.* We also recommend that you review the identity theft materials posted for consumers on the Federal Trade Commission's (the "FTC's") Web site, [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/), and in particular, the posted copy of the FTC's booklet, *"Take Charge: Fighting Back Against Identity Theft."*

We are reaching out to assist those former clients who may have been affected by this unfortunate incident:

- Should you have any questions about this incident or need additional information, please contact us at the special number we have set up for you, **1-800-736-6153**.
- We would like to offer you, at our expense, a one-year enrollment to Experian's Triple Advantage<sup>SM</sup> three-bureau credit monitoring product to help you begin the process of regularly reviewing your account records for any abnormalities. If you choose to enroll in the membership, please contact us at the toll-free number above and our representatives will help enroll you.

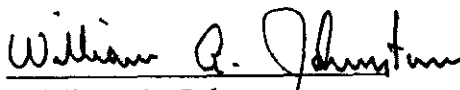
We also have contacted the three principal credit reporting bureaus, Equifax, Experian and TransUnion, to advise them of the situation.

We regret the occurrence of this incident and any inconvenience it may have caused you. If you have further questions or concerns, please do not hesitate to call the toll-free number referred to above.

Sincerely,



Ian B. Davidson  
Chairman



William A. Johnstone  
President and CEO

### Steps to take to protect your credit and identity

Should you ever believe your identity has been stolen or that you are at risk of having your identity stolen, you can follow the Federal Trade Commission's ("FTC's") guidelines on protecting yourself against identity theft. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them.

First, you should contact your credit and bank card issuers as soon as possible to review your accounts for unauthorized charges or transactions. If there are unauthorized charges or if you otherwise believe that your card number has been taken by an unauthorized person, you should inform your card issuer on the phone and in writing that the charges were not authorized by you, and you should request that your current card account be closed and a new card issued in your name.

You may wish to consider placing a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing credit accounts. Because creditors seek additional verification from you when a fraud alert is in place on your credit file, one effect of the fraud alert is that it slows the processing time for opening new accounts and making changes on your existing accounts.

To place a fraud alert on your credit file, call any one of the three major credit bureaus. As soon as one credit bureau processes your fraud alert, it will notify the other credit bureaus on your behalf to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax  
1-800-525-6285

Experian  
1-888-397-3742

TransUnionCorp  
1-800-680-7289

You may also have right under applicable state law to request a "security freeze" on your credit report. A security freeze will prohibit a credit reporting agency from releasing any information in your credit report without your express authorization.

Even if you do not initially find any suspicious activity on your card accounts, credit reports and/or bank statements, the FTC recommends that you check your credit reports, card charges and financial statements regularly. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports, card charges and financial statements periodically can help you spot problems and address them quickly. Once a year you can obtain a free credit report by calling 1-877-322-8228 or going online to [www.annualcreditreport.com](http://www.annualcreditreport.com).

If you find suspicious activity on your accounts or have reason to believe that your personal information is being misused, it may be necessary for you to file a police report and obtain a copy of that police report. Many creditors require the information the police report contains to absolve you of the fraudulent debts.

You may also want to file a complaint with the FTC, which will be logged into its database of identity theft cases used by law enforcement agencies for investigations. To get free information or file a complaint with the FTC, you may call the FTC at 1-877-438-4338, or use the complaint form at <http://www.consumer.gov/idtheft/>.