



Brenda R. Sharton
+1 617 570 1214
bsharton@goodwinlaw.com

Goodwin Procter LLP
100 Northern Avenue
Boston, MA 02210

goodwinlaw.com
+1 617 570 1000

June 18, 2018

VIA FEDEX

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We write on behalf of Manchester Capital Management, LLC ("MCM") to notify you that in late May 2018, after forensic analysis, MCM determined that certain personal information belonging to New Hampshire residents was on computer hardware that had been previously stolen from MCM's offices.

Specifically, in May 2017, MCM's Montecito, California office was burglarized. During the burglary, intruders vandalized the facilities and stole a number of items, including some bicycles belonging to MCM employees and a piece of computer hardware. MCM promptly reported the matter to the Santa Barbara Police Department, and independent analysis at the time indicated that there was no confidential information on the missing hardware. After nearly a year of investigating the break-in, law enforcement identified the perpetrator and ultimately was able to successfully recover the stolen equipment. Immediately after law enforcement turned the hardware over to MCM, MCM launched a forensic review of the recovered hardware, and found personal information belonging to certain New Hampshire residents that may have been viewed by an unauthorized person while it was not in MCM's custody.

The affected information may include names, account numbers, and social security numbers of MCM clients and employees. MCM has identified 2 New Hampshire residents potentially impacted by the incident. At this time MCM does not have any evidence that any MCM client or employee has been subject to identity theft or fraud as a result of the incident.

MCM would like to emphasize that this incident did not involve an unauthorized intrusion into its computer systems through the Internet. The computer hardware and information contained on it was obtained through a physical intrusion into MCM's office space. MCM is nevertheless reviewing its security posture to help protect against a similar event occurring in the future.

MCM is taking prompt action to assist New Hampshire residents who may be impacted by this event. MCM notified potentially affected individuals, and recommended actions they can take to protect themselves, such as monitoring account statements, obtaining credit reports, and instituting a security freeze on their credit files. MCM also is making available to all potentially affected individuals 24

STATE
DEPT OF
2018 JUN 19 AM 8:1



June 18, 2018
Page 2

months of identity theft protection services from AllClear ID, at no cost to the individuals. A template copy of the notification letter that MCM sent to New Hampshire residents on June 13, 2018 is attached to this notice.

Thank you for your attention to this matter.

Sincerely,

A handwritten signature in blue ink that reads "Brenda R. Sharton".

Brenda R. Sharton

BRS

June 12, 2018

Client
123 Any Street
Anytown, US 00000

Dear Client,

We write to notify you of a burglary that occurred at the Montecito, California office of Manchester Capital Management, LLC ("MCM"). Please review this letter carefully to learn about the incident and how it may affect you.

What Happened?

In May 2017, MCM's Montecito, California office was burglarized. The intruders vandalized the facilities and stole a piece of computer hardware along with some bicycles and other personal items belonging to MCM employees. MCM promptly reported the matter to the Santa Barbara Police Department, which opened an investigation into the break-in. At the time, MCM had no evidence that any information was on the stolen hardware. After nearly a year of investigating, law enforcement identified the perpetrator and successfully recovered the stolen equipment. Immediately after law enforcement turned the hardware over to MCM, MCM launched a review into what was on the hardware. After analysis, MCM discovered that certain client and employee information was on the hardware and may have been viewed by an unauthorized person while it was not in MCM's custody. Because we identified sensitive information on the stolen hardware, we are sending this letter to all past and present MCM clients and employees.

While this is a data breach notice, we want to emphasize that there was no unauthorized intrusion onto our computer systems through the internet. This was a burglary of our physical office in Montecito in which the perpetrator stole items that included the computer hardware.

What Information Was Involved?

The affected information may include names, account numbers, and social security numbers. We are sending you this notice as a precaution and to encourage you to take steps to monitor your personal information. At this time, we do not have any evidence that any MCM client, employee, or related party has been subject to identity theft or fraud as a result of this burglary.

What We Are Doing

MCM takes this issue very seriously. Accordingly, we have retained AllClear ID, a specialist in identity theft protection, to provide you with 24 months of identity theft protection services free of charge should you choose to enroll. Instructions for accessing these services are below.

What You Can Do

As always, we recommend that you remain vigilant for incidents of fraud and identity theft, including regularly viewing your account statements and monitoring your free credit reports.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy.

To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling (877) 676-0379 using the following redemption code(s): CODE FIELD.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call (877) 676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

If you would like, or believe you need, additional enrollment codes for other members of your household, please call MCM at (802) 362-4410 for assistance.

For more information on how you can help protect yourself, please review the enclosed *Steps You Can Take to Protect Yourself from Identity Theft*.

For More Information

If you have any further questions or concerns about this incident, feel free to contact your wealth manager, or Bart Kraft at (802) 362-4410 or BKraft@mcmlc.com.

We thank you for your patience and understanding as we work through this unfortunate incident.

Sincerely,



Drew Beresford
President

Steps You Can Take to Protect Yourself from Identity Theft

1. *Review your account statements and credit reports and notify law enforcement and MCM of suspicious activity.*

Even if you do not feel the need to register for a credit monitoring service, as a precautionary measure, we recommend that you regularly review statements from your bank, credit card, and other accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies:

Equifax

P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
1.888.766.0008

Experian

P.O. Box 9532
Allen, TX 75013
www.experian.com
1.888.397.3742

TransUnion

P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com
1.800.680.7289

When you receive your credit reports, look them over carefully. Look for accounts that you did not open and/or inquiries from creditors that you did not initiate. Also check to see if your personal information on the credit report is accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend that you remain vigilant in your review of your account statements and credit reports. You should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission.

2. *Consider placing a fraud alert or a security freeze on your credit files.*

Fraud Alerts: There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed above.

Security Freezes: You may have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze,

potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Security freeze laws vary from state to state.

Keep in mind that when you place the freeze, you may not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. In addition, you may incur fees to place, lift and/or remove a credit freeze. The cost of placing, temporarily lifting, and removing a security freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies at the numbers above to find out more information.

3. *Learn more about how to protect yourself from identity theft.*

You may wish to review the Federal Trade Commission's guidance on how consumers can protect themselves against identity theft. For more information:

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580
www.ftc.gov/idtheft
1.877.ID.THEFT (1.877.438.4338)

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

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

For residents of Massachusetts: Under Massachusetts law, you have the right to obtain a police report filed in regard to this incident, if one was filed. A copy of a police report may be required by creditors to clear up your records.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov