

RECEIVED

DEC - 9 2013

OFFICE OF CONSUMER PROTECTION  
INVESTIGATIONS



November 27, 2013

Lori Nugent  
312.821.6177 (direct)  
Lori.Nugent@wilsonelser.com

Office of Consumer Protection  
Leiopapa A Kamehameha Building  
235 South Beretania Street, Suite 801  
Honolulu, Hawaii 96813

To Whom It May Concern:

We represent Maricopa County Community College District ("MCCCD") with respect to a security incident involving the potential exposure of certain personal information described in detail below. MCCCD is a community college district comprised of 10 separate community colleges, two skill centers, and a District office located in Maricopa County, Arizona.

MCCCD takes the security of the information in its control very seriously. Accordingly, it has taken steps to identify individuals whose sensitive data may have been exposed in the incident discussed below, and provide appropriate services to them including continuous credit monitoring and enhanced identity theft consultation and restoration. Mailing of notification letters to these individuals is commencing today. At present there is no indication that the information has been inappropriately accessed, misused or further disclosed. MCCCD also has taken steps to prevent this type of incident from occurring in the future.

Since MCCCD is based in Maricopa County, Arizona, the overwhelming majority of individuals who will be receiving notification letters reside in Arizona. We note that MCCCD has informed the Arizona Auditor General's Office of this situation and has provided extensive briefing to this regulatory body. MCCCD also has provided extensive briefing to the Higher Learning Commission, which has stated that MCCCD "is doing an excellent job in addressing this situation."

The remainder of this letter provides further information about this situation.

## 1. Nature of Unauthorized Access

### A. Overview of Security Incidents

#### i. *2011 Security Incident*

In January 2011, the FBI informed a MCCCD Information Technology Services ("ITS") employee that one or more of MCCCD's databases were available for sale on the Internet.

MCCCD personnel conducted an internal investigation in response to that security incident, followed by an investigation by outside security consultants, Stach & Lui (now Bishop Fox). As discussed below, certain MCCCD employees withheld information and obstructed the investigation into the 2011 security incident, which effectively deprived MCCCD of knowledge of security vulnerabilities. This employee conduct did not meet MCCCD's standards and expectations, and ultimately caused the 2013 security incident.

ii. *2013 Security Incident*

On April 29, 2013, the FBI informed MCCCD that fourteen of its databases, which were located on MCCCD web servers, were listed for sale on a website. MCCCD ITS immediately took the identified servers offline, stopped all web development in the current web environment, and initiated an internal review of its entire system. In May of 2013, while investigating the 2013 security incident, MCCCD management learned that, in response to the 2011 security incident, Stach & Lui had issued a report to certain MCCCD employees identifying significant security vulnerabilities. A copy of the 2011 Stach & Lui report was obtained, and executive leadership was informed for the first time of the report. In response, MCCCD retained Wilson Elser as outside counsel, and through counsel, retained Kroll Advisory Services ("Kroll"), to assist with two investigations, the first into the District and Colleges' web servers, and second into employee conduct and the second. The investigation results showed that some of MCCCD's ITS employees had engaged in conduct that was not consistent with MCCCD's standards and expectations. This conduct ultimately led to the 2011 and 2013 network security incidents. The results of the investigation, and the steps taken by MCCCD in response, are summarized below.

B. Employment Investigation and Responsive Measures Taken

Under direction of counsel, Kroll conducted an independent investigation of employee conduct in connection with the 2013 and 2011 network security incidents. Kroll's investigation included an analysis of the MCCCD network; documentation and correspondence regarding the security incidents; interviews of current and former MCCCD ITS employees responsible for the networks and/or any remedial responses taken; and interviews of outside security consultants retained to assist in the investigation of the security incidents. On November 19, 2013 Kroll issued its independent report, which found that employee conduct did not meet Maricopa standards and expectations. Employment action by MCCCD against these employees is underway, in accordance with these recommendations and MCCCD employment policies and procedures, in compliance with Arizona law.

C. Forensic Investigation and Responsive Measures Taken

As noted above, MCCCD engaged Kroll through counsel to forensically review the District and Colleges' servers, analyze the information obtained, and determine whether any sensitive data may have been accessed by an unauthorized individual investigation that involved multiple servers and systems and extensive review of data over several months. On October 18, 2013, Kroll completed its investigation, which found that because of extensive remediation efforts taken by MCCCD immediately after April 2013 event, Kroll was unable to determine whether any sensitive data was exfiltrated from MCCCD's systems. While there was no evidence of exfiltration, sensitive information contained in MCCCD's systems could have been accessed

without authorization. In this context, MCCCCD decided to provide notification, credit monitoring, and identity theft restoration services to all individuals whose information *may* have been accessed.

MCCCCD's systems contained sensitive information of MCCCCD students, employees, and vendors. Employee information contained in the system included the following information: names, addresses, phone numbers, e-mail addresses, Social Security Numbers, dates of birth, financial and bank account information, certain demographical information, information related to employment, education and training, and limited benefits information, including plan selection, vacation accrual, or dependent's information. The systems contained the following information pertaining to MCCCCD's students: names, addresses, phone numbers, e-mail addresses, Social Security Numbers, dates of birth, certain demographical information, and enrollment, academic, and financial aid information. Vendor information included names, business names, addresses, Federal Employer Identification Number, and bank account information.

MCCCCD worked with Kroll to extract the information necessary to provide notification to individuals and businesses whose sensitive data was exposed. Notification is being provided commencing today.

#### D. Steps Taken in Response to the Security Incidents

As noted above, high-level management at MCCCCD was not aware of the initial security incident that occurred in 2011 due to material omissions and/or misstatements of fact made by certain employees. As soon as this situation was brought to the attention of high-level management in 2013, the Chancellor took immediate action to secure the web environment implement increased security controls, increase accountability of IT employees, and ensure that privacy and security are a top MCCCCD priority, incorporated by design into all IT work. For your convenience, a summary timeline of events as well as the steps taken as a result of the 2013 situation is provided as follows:

- April 29, 2013 – June 14, 2013
  - MCCCCD was notified by the FBI that a website known for highlighting security vulnerabilities had identified MCCCCD's website, [www.maricopa.edu](http://www.maricopa.edu), as being unsecure. The website indicated that they had 140 MCCCCD databases for sale. The FBI subsequently informed MCCCCD that only 14 (not 140) databases may have been compromised. On May 6, 2013, the FBI informed MCCCCD that no information contained in the databases appears to have been released. MCCCCD's internal investigation initially found that only three of the potentially affected databases may have been compromised.
  - MCCCCD took the affected servers/databases offline, commenced an internal investigation into this situation, and MCCCCD sought outside assistance in identifying and containing the security incident, contracting with Stach and Liu to assist with security improvements for current and future web development.

- New hardware and software was installed to more securely host the current web environment, and a Palo Alto Web Application Firewall (“WAF”) device was installed to “front-end” the current web environment. The MCCCDD web server was brought back online with these new security enhancements in place.
- June 15, 2013 – August 30, 2013
  - MCCCDD engaged Eagle Creek, a web development firm, to lead and assist in the daily maintenance of the current web environment.
  - MCCCDD retained Kroll, an independent forensic investigation consultant, to forensically review the District and Colleges’ servers, analyze the information obtained, and reach a determination with respect to what data, if any, was exposed.
  - MCCCDD implemented the One Maricopa Network Enhancement (“OMNE”) initiative, making data security and privacy Job #1 by enhancing the security of the District website, aligning websites across the District, improving Maricopa's network, and ensuring that all IT work incorporates privacy and security.
  - A Breach Response Team (“BRT”) commenced meetings to assist the executive team in accomplishing action items related to the investigation.
  - Two college CIOs were tasked to assist District ITS as Co-CIOs to manage the ITS operation, enhancing data security and privacy while integrating and improving ITS operations, reporting directly to the Chancellor.
- September 01, 2013 – October 31, 2013
  - MCCCDD continued prioritizing IT projects, and at the direction of the Chancellor, significant strategic projects are put on hold until privacy and security work is completed.
  - MCCCDD installed and configured an Oracle Database Firewall to monitor the incoming and outgoing database communications with MCCCDD’s student information system (“SIS”).
  - MCCCDD obtained quotes from three breach response vendors, and ultimately contracted with Kroll to provide for data collection, notification, call center, credit monitoring, and identity theft restoration services.
- November 01, 2013 – November 26, 2013
  - MCCCDD implemented shunning technology and risk tools to block traffic to and from “at risk” IP addresses and providing a controlled way of notifying, alerting, and educating employees on MCCCDD’s policies and practices in creating a safe and secure technology environment.
- November 27, 2013
  - Mailing of notification letters commenced.

If it would be useful, we are happy to further discuss the remedial measures that have been taken to address this situation.

## 2. Number of Hawaii residents affected

Notification is being provided to 3,678 Hawaii residents whose information may have been contained on MCCCCD's systems. A copy of the notification letter is attached to this letter.

## 3. Steps taken or planned relating to the incident

MCCCCD has taken numerous steps designed to prevent this type of situation from happening again, including initiating employment action against those ITS employees whose inappropriate conduct allowed vulnerabilities to exist within the IT system and resulted in the 2011 and 2013 security incidents. MCCCCD has conducted a comprehensive review of its ITS department, and is in the process of reconfiguring its IT structure to ensure increased accountability, using checks and balances in its structure, including Interim Co-CIOs reporting directly to the Chancellor. As part of this process, it also has created a Chief Information Security Officer position, for which it is currently accepting applications.

MCCCCD has also installed several new firewalls to control the flow of information between its systems and the internet. State-of-the-art shunning technology, which blocks communications to and from "at risk" IP addresses has been deployed, and is effectively shunning efforts to access MCCCCD's systems. Additionally, MCCCCD has implemented tools that will allow it to more effectively monitor its systems, and is in the process of revising its security policies. MCCCCD is in the process of redesigning its Web environment to implement additional security measures, and has aligned all IT projects under the One Maricopa Network Enhancement Initiative to ensure that privacy and security remains Job # 1.

Through Kroll, MCCCCD is providing individuals whose information *may* have been accessed without authorization with one year of continuous credit monitoring and enhanced identity theft consultation and restoration services at no cost to the individual. At present there is no indication that the information has been inappropriately accessed, misused or further disclosed.

## 4. Other notification and contact information

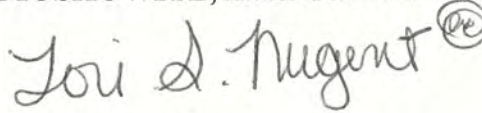
Notification has been provided to the Consumer Reporting Agencies.

\* \* \*

MCCCCD takes the security and privacy of the information in its control very seriously, and has taken steps to prevent this type of incident from occurring in the future. Should you have any questions or concerns, or require additional information, please do not hesitate to contact me.

Very truly yours,

**WILSON, ELSER, MOSKOWITZ, EDELMAN & DICKER LLP**

*Lori S. Nugent* 

Lori S. Nugent

cc: Cynthia D. Shenker, Wilson Elser  
Gerald J. Jennings, Wilson Elser  
Melissa K. Ventrone, Wilson Elser



Your membership number is: <<MEMBERSHIPNUMBER>>  
 Go to [www.idintegrity.com](http://www.idintegrity.com) to start your credit monitoring  
 Call 1-855-330-6366 if you need help or have questions  
 8 a.m. to 5 p.m. (Central Time), Monday through Friday  
 To receive credit monitoring, 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.

<<Firstname>> <<Middlename>> <<Lastname>>  
 <<Address1>>  
 <<Address2>>  
 <<City>>, <<Stateprovince>> <<Postalcode>>  
 <<Intelligent Mail Barcode>>

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

Dear <<Firstname>> <<Middlename>> <<Lastname>>,

We are writing to inform you of a security incident that may have resulted in the disclosure of your personal information. While we are not aware at this time of any misuse of anyone's information, we are providing resources to assist you and answer any questions you may have. We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this may cause you.

**What Happened?**

We recently discovered that Maricopa County Community Colleges District IT systems may have been accessed without authorization, and we are cooperating with law enforcement officials investigating the matter. On October 18<sup>th</sup>, 2013, we determined that your information, including your name, address, phone number, e-mail address, Social Security number, date of birth, financial and bank account information, certain demographical information, information related to your employment, education and training, and limited benefits information such as your plan selection, vacation accrual, or dependent's information may have been accessed without authorization. The systems did not contain credit card information or personal health information.

Immediately after learning of this situation, we initiated a thorough investigation, including engaging independent data forensics experts. We have taken steps to enhance our systems, and implemented measures designed to prevent this type of event from happening again. This includes installing a new firewall, installing additional monitoring services, reviewing our access list, reviewing our policies and procedures, and applying other increased security controls.

**Resources Available to You**

Although we are not aware of any misuse of your information, out of an abundance of caution, we have hired Kroll Advisory Solutions to provide identity safeguards and other services at no cost to you for one year through its ID TheftSmart™ program. Your safeguards include Continuous Credit Monitoring and Enhanced Identity Theft Consultation and Restoration. Instructions on how to receive your services are attached.

We sincerely regret any inconvenience or concern that this matter may cause. If you have any questions regarding this incident, Kroll's experts are standing by to assist you Monday through Friday from 8 a.m. to 5 p.m. Central Time, and can be reached by calling toll-free (855) 330-6366. We remain committed to protecting the security of your personal information.

Sincerely,

Rufus Glasper, Ph.D., CPA  
 Chancellor

## Continuous Credit Monitoring

*Early Detection is Key*

Consumer and government agencies recommend that you keep a close eye on your credit activity. Frequent monitoring is key to identifying fraud and reducing the damage it can cause. Monitoring alerts make you aware of changes in your credit file that could indicate identity theft and fraud.

You'll be notified by email when your credit files are updated with certain credit activity that could be associated with identity theft, such as applying for a new credit card or loan, a change of address, and more. If any activity looks suspicious, simply call us toll-free. We'll immediately put you in touch with your Licensed Investigator to find out what's happening and help take measures to correct the problem. We'll even send you notices when there's been no activity in your credit file, so you always know your credit is closely monitored.

**Go to [www.idintegrity.com](http://www.idintegrity.com) to start your complimentary Credit Monitoring.**

**To receive your credit monitoring by mail instead of online, please call 1-855-330-6366.**

## Enhanced Identity Theft Consultation and Restoration

*Restore Your Credit, Regain Your Peace of Mind*

You can rely on the expertise of a specialized team of investigators to help search out suspicious activity and fight back against the evolving tactics used by identity thieves. Our Licensed Investigators have thousands of hours of experience working with and utilizing the laws, regulations, and investigative techniques used for identity theft restoration.

Our consultation services allow you to minimize your risk if your personal data has been compromised. Our tenured investigators can give you personal one-on-one consultation on how best to reduce your identity theft risk. Additionally, if you are a victim of identity theft, we provide full-service restoration, which means experienced Licensed Investigators do the heavy lifting to restore your identity on your behalf. And since one dedicated investigator is assigned to your case, you can rest assured you will receive the individualized, personal support that is critical to recovering from identity theft.

You now have easy access to the resources you need to search out suspicious activity and to fight back if you have been exposed to the threat of identity fraud.

**If you have an identity theft issue or if you have any questions,  
Call 1-855-330-6366, 8 a.m. to 5 p.m. (Central Time), Monday through Friday.  
Your Licensed Investigator is ready to help you.**

## State Notification Requirements

### All States.

You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 <a href="http://www.equifax.com">www.equifax.com</a>	P.O. Box 2104 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	P.O. Box 2000 Chester, PA 19022 1-800-888-4213 <a href="http://www.transunion.com">www.transunion.com</a>

### For residents of Massachusetts.

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

### For residents of Massachusetts and West Virginia.

You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that 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) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address,

and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

### For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

### For residents of Iowa.

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

### For residents of Oregon.

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

### For residents of Illinois, Maryland and North Carolina.

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about steps you can take toward preventing identity theft.

### 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](http://www.oag.state.md.us)

### North Carolina Office of the Attorney General

Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
[www.ncdoj.com](http://www.ncdoj.com)

### Federal Trade Commission Consumer Response Center

600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)





MARICOPA  
COMMUNITY  
COLLEGES®

Your membership number is: <<MEMBERSHIPNUMBER>>  
Go to [www.idintegrity.com](http://www.idintegrity.com) to start your credit monitoring  
Call 1-855-330-6366 if you need help or have questions  
8 a.m. to 5 p.m. (Central Time), Monday through Friday  
To receive credit monitoring, 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.

<<Firstname>> <<Middlename>> <<Lastname>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<Stateprovince>> <<Postalcode>>  
<<Intelligent Mail Barcode>>

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

Dear <<Firstname>> <<Middlename>> <<Lastname>>,

We are writing to inform you of a security incident that may have resulted in the disclosure of your personal information. While we are not aware at this time of any misuse of anyone's information, we are providing resources to assist you and answer any questions you may have. We take the security of your personal information very seriously, and sincerely apologize for any inconvenience this may cause you.

**What Happened?**

We recently discovered that Maricopa County Community Colleges District IT systems may have been accessed without authorization, and we are cooperating with law enforcement officials investigating the matter. On October 18<sup>th</sup>, 2013, we determined that your information, including your name, address, phone number, e-mail address, Social Security number, date of birth, certain demographical information, and enrollment, academic and financial aid information may have been accessed without authorization. The systems did not contain credit card information or personal health information.

Immediately after learning of this situation, we initiated a thorough investigation, including engaging independent data forensics experts. We have taken steps to enhance our systems, and implemented measures designed to prevent this type of event from happening again. This includes installing a new firewall, installing additional monitoring services, reviewing our access list, reviewing our policies and procedures, and applying other increased security controls.

**Resources Available to You**

Although we are not aware of any misuse of your information, out of an abundance of caution, we have hired Kroll Advisory Solutions to provide identity safeguards and other services at no cost to you for one year through its ID TheftSmart™ program. Your safeguards include Continuous Credit Monitoring and Enhanced Identity Theft Consultation and Restoration. Instructions on how to receive your services are attached.

We sincerely regret any inconvenience or concern that this matter may cause. If you have any questions regarding this incident, Kroll's experts are standing by to assist you Monday through Friday from 8 a.m. to 5 p.m. Central Time, and can be reached by calling toll-free (855) 330-6366. We remain committed to protecting the security of your personal information.

Sincerely,

Rufus Glasper, Ph.D., CPA  
Chancellor

## Continuous Credit Monitoring

*Early Detection is Key*

Consumer and government agencies recommend that you keep a close eye on your credit activity. Frequent monitoring is key to identifying fraud and reducing the damage it can cause. Monitoring alerts make you aware of changes in your credit file that could indicate identity theft and fraud.

You'll be notified by email when your credit files are updated with certain credit activity that could be associated with identity theft, such as applying for a new credit card or loan, a change of address, and more. If any activity looks suspicious, simply call us toll-free. We'll immediately put you in touch with your Licensed Investigator to find out what's happening and help take measures to correct the problem. We'll even send you notices when there's been no activity in your credit file, so you always know your credit is closely monitored.

**Go to [www.idintegrity.com](http://www.idintegrity.com) to start your complimentary Credit Monitoring.**

**To receive your credit monitoring by mail instead of online, please call 1-855-330-6366.**

## Enhanced Identity Theft Consultation and Restoration

*Restore Your Credit, Regain Your Peace of Mind*

You can rely on the expertise of a specialized team of investigators to help search out suspicious activity and fight back against the evolving tactics used by identity thieves. Our Licensed Investigators have thousands of hours of experience working with and utilizing the laws, regulations, and investigative techniques used for identity theft restoration.

Our consultation services allow you to minimize your risk if your personal data has been compromised. Our tenured investigators can give you personal one-on-one consultation on how best to reduce your identity theft risk. Additionally, if you are a victim of identity theft, we provide full-service restoration, which means experienced Licensed Investigators do the heavy lifting to restore your identity on your behalf. And since one dedicated investigator is assigned to your case, you can rest assured you will receive the individualized, personal support that is critical to recovering from identity theft.

You now have easy access to the resources you need to search out suspicious activity and to fight back if you have been exposed to the threat of identity fraud.

**If you have an identity theft issue or if you have any questions,  
Call 1-855-330-6366, 8 a.m. to 5 p.m. (Central Time), Monday through Friday.  
Your Licensed Investigator is ready to help you.**

## State Notification Requirements

### All States.

You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
P.O. Box 740241 Atlanta, GA 30374 1-800-685-1111 <a href="http://www.equifax.com">www.equifax.com</a>	P.O. Box 2104 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	P.O. Box 2000 Chester, PA 19022 1-800-888-4213 <a href="http://www.transunion.com">www.transunion.com</a>

### For residents of Massachusetts.

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

### For residents of Massachusetts and West Virginia.

You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that 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) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address,

and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

### For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

### For residents of Iowa.

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

### For residents of Oregon.

State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

### For residents of Illinois, Maryland and North Carolina.

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about steps you can take toward preventing identity theft.

### 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](http://www.oag.state.md.us)

### North Carolina Office of the Attorney General

Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
[www.ncdoj.com](http://www.ncdoj.com)

### Federal Trade Commission Consumer Response Center

600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
[www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)