

RECEIVED

JAN 18 2018

CONSUMER PROTECTION

Michael J. Waters
Shareholder
+1 312 609 7726
mwaters@vedderprice.com

January 16, 2018

**VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
AND FEDERAL EXPRESS**

The Honorable Gordon MacDonald
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of a Potential Breach of Security Involving Computerized Data Containing Personal Information Pursuant to N.H. REV. STAT. ANN. § 359-C:20

Dear Attorney General MacDonald:

We represent Pension Fund of the Christian Church ("Pension Fund") in connection with two incidents that involved the personal information of some New Hampshire residents, and provide this notice on behalf of Pension Fund pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Pension Fund is notifying you of these incidents, Pension Fund does not waive any rights or defenses relating to the incidents or this notice, or the applicability of New Hampshire law or personal jurisdiction in connection with this incident.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On December 11, 2017, Pension Fund learned that a text file was accessed without authorization and that the text file contained certain members' personal identification information. It discovered this as part of an investigation it undertook after it appeared a legacy computer server had been used for the mining of crypto currency. There is no evidence that the file was ever copied or exfiltrated from the server. Nevertheless, because the file was accessed and contained members' personal information, including names, dates of birth, Social Security numbers and member identification numbers, Pension Fund is providing notice to all potentially impacted members.

In addition, on December 18, 2017, Pension Fund learned that a password protected employee laptop had been stolen from a locked car and that the laptop contained certain personal information of members, including members' names, date of birth, addresses, account numbers, Social Security numbers, and member identification numbers.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

It was determined that 19 New Hampshire residents may have been impacted in total. There is significant overlap in the population of residents impacted by both incidents. The crypto currency mining incident impacted 19 New Hampshire residents. The incident involving the stolen laptop

impacted 11 New Hampshire residents. Pension Fund will be notifying impacted individuals of the situation by letter on January 16, 2018. Enclosed is a copy of the notice that is being sent to the impacted individuals.

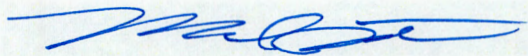
STEPS TAKEN RELATING TO THE INCIDENTS

Upon learning of the crypto currency mining incident, Pension Fund secured its systems, retained a leading cybersecurity firm to perform a forensic investigation, and contacted federal law enforcement. It is working with law enforcement as it conducts its investigation. Upon learning of the stolen laptop, Pension Fund took steps to encrypt all employee laptops. Pension Fund is also providing free identity theft protection services to the impacted individuals through Experian.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

A handwritten signature in blue ink, appearing to read "M. Waters", is written over a light blue rectangular background.

Michael J. Waters
Shareholder



Pension Fund

of the Christian Church
strong. smart. secure.

NOTICE OF DATA BREACH

Pension Fund of the Christian Church values and respects your privacy, which is why we are writing to advise you about two recent incidents that may affect your personal information, to explain the steps that we have undertaken since discovering the incidents and to provide you with guidance on what you can do to protect yourself.

What Happened

As we previously communicated to our membership, Pension Fund recently became aware of a potential unauthorized access to one of its legacy servers. Promptly upon discovering the situation, we launched an investigation and retained a leading forensic firm to assist with the investigation. On December 11, 2017, we learned that a text file that appears to have been accessed without authorization contained the personal information of some of our members. At this time, we have no evidence that any information in the file was copied or sent from the server, but because the file was accessed and it contained member information, we are making all members aware of the situation.

In addition, on December 18, 2017, Pension Fund learned that a password protected employee laptop had been stolen from a locked car and that the laptop contained members' personal information.

What Information Was Involved

The legacy server file included some members' names, dates of birth, Social Security numbers, and member identification number (PIN). The laptop contained members' names, date of birth, addresses, account numbers, Social Security numbers, and PIN.

What We Are Doing

Once we learned of the unauthorized access of the legacy server, we moved quickly to secure our systems and sensitive information. In addition to our own internal investigation, we retained a leading cybersecurity forensics firm and contacted law enforcement, and continue to work closely with them as they conduct their ongoing investigation. As it relates to the stolen laptop, the device is password protected and remote monitoring software has been set up to monitor for a connection to the stolen device, and should it occur, an automated attempt will be made to connect to the machine and erase its contents.

What You Can Do

To help protect your information, we encourage you to take advantage of the complimentary one-year credit monitoring and identity protection services we are offering you through Experian's IdentityWorksSM Credit 3B. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. The Experian IdentityWorksSM Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and the Experian IdentityWorksSM Credit 3B, please see the additional information provided with this letter.**

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identify theft by, among other things, 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 incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by 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 can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

| | | |
|------------------------------------------------------|--------------------------------------------------------|------------------------------------------------------------|
| Equifax | Experian | TransUnion |
| 1-800-349-9960 | 1-888-397-3742 | 1-888-909-8872 |
| www.equifax.com | www.experian.com | www.transunion.com |
| P.O. Box 105788 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19022 |

Fraud Alerts: 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 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

Credit and Security Freezes: You may have the right to put a credit freeze, also known as a security 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit 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 credit 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 as specified below to find out more information:

Equifax Security
Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security
Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834

You can obtain more information about the fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

This notice has not been postponed at the request of a law enforcement agency; however, we did communicate with law enforcement prior to issuing this notice.

Iowa Residents: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
and on-line at <http://www.iowaattorneygeneral.gov>

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft at:

Office of the Attorney General
220 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.com

Rhode Island Residents: We believe that these incidents affected nine Rhode Island residents. You can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400

For More
Information

We apologize for any inconvenience or concern that these incidents might cause you. Should you have any questions, please feel free to call Todd Adams at 1-866-495-7322 between 9:00 a.m. and 5:00 p.m., Eastern time, Monday through Friday.

Activating Your Complimentary Credit Monitoring

To help protect your identity, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **April 15, 2018** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code: ABC123**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [engagement number] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

1. **Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

**Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and is intended for informational purposes only, and it does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.



Pension Fund

of the Christian Church
strong. smart. secure.

We are writing to notify you of two recent incidents that may have involved the disclosure of certain of your personal information. While we have no reason to believe that any of the information has been or will be used for any improper purpose, we value and respect your privacy and want to advise you of steps you can take to protect your identity.

We learned of the incidents on December 11 and 18, 2017 and subsequently determined that certain of your personal information may have been impacted, including your name, or a portion of your name, date of birth, address, account number, Social Security number, and member identification number (PIN). As a result, we are providing you with this notice and information on steps you can take to help protect yourself and your personal information.

We arranged and want to encourage you to take advantage of the complimentary one-year credit monitoring and identity protection services we are offering you through Experian's® ProtectMyID® Alert. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided with this letter.**

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identify theft by, among other things, 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 incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. *Take Charge: Fighting Back Against Identity Theft*, a comprehensive guide from the FTC to help you guard against and deal with identity theft, may be found on the FTC's website at <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idtheft04.shtm>.

We recommend that you regularly review statements from your 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 listed at the bottom of this page.

You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Fraud Alerts: There are also 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 ask 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 contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Credit Freezes: You may have the right to put a credit freeze, also known as a security 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 credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit 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 credit 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 as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com)
P.O. Box 105851
Atlanta, GA 30348
800-685-1111

Fraud Alerts:

P.O. Box 105069, Atlanta, GA 30348

Credit Freezes:

P.O. Box 105788, Atlanta, GA 30348

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:

P.O. Box 9554, Allen, TX 75013

TransUnion
(www.transunion.com)
P.O. Box 105281
Atlanta, GA 30348
877-322-8228

Fraud Alerts and Security Freezes:

P.O. Box 2000, Chester, PA
19022
888-909-8872

Under Massachusetts law, you also have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Should you have any questions, please feel free to call Todd Adams at 1-866-495-7322 between 9:00 a.m. and 5:00 p.m., Eastern time, Monday through Friday.

Activating Your Complimentary Credit Monitoring

To help protect your identity, we are offering a complimentary one-year membership of Experian's® ProtectMyID® Alert.. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate ProtectMyID Now in Three Easy Steps

1. **ENSURE That You Enroll By: April 15, 2018** (Your code will not work after this date.)
2. **VISIT the ProtectMyID Web Site to enroll:** <https://www.experianidworks.com/3bcredit>
3. **PROVIDE Your Activation Code: ABC123**

If you have questions or need an alternative to enrolling online, please call 1-877-288-8057 and provide engagement #[engagement number].

ADDITIONAL DETAILS REGARDING YOUR ONE-YEAR PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
 - **Daily Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution and ProtectMyID ExtendCARE:** Toll-free access to U.S.-based customer care and a dedicated Identity Theft Resolution agent, who will walk you through the process of fraud resolution from start to finish for seamless service. The agent will investigate each incident; help you contact credit grantors to dispute charges and close accounts, including credit, debit and medical insurance cards; assist with freezing credit files; and contact government agencies.
 - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance:** Immediately covers certain costs, including lost wages, private investigator fees and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 1-877-288-8057.



Pension Fund

of the Christian Church

strong. smart. secure.

NOTICE OF DATA BREACH

Pension Fund of the Christian Church values and respects your privacy, which is why we are writing to advise you about two recent incidents that may affect the personal information of your deceased family member.

What Happened

Pension Fund recently became aware of a potential unauthorized access to one of its legacy servers. Promptly upon discovering the situation, we launched an investigation and retained a leading forensic firm to assist with the investigation. On December 11, 2017, we learned that a text file that appears to have been accessed without authorization contained the personal information of some of our members. At this time, we have no evidence that any information in the file was copied or sent from the server, but because the file was accessed and it contained member information, we are making all members aware of the situation.

In addition, on December 18, 2017, Pension Fund learned that a password protected employee laptop had been stolen from a locked car and that the laptop contained members' personal information.

What Information Was Involved

The legacy server file included some members' names, dates of birth, Social Security numbers, and member identification number (PIN). The laptop contained members' names, date of birth, addresses, account numbers, Social Security numbers, and PIN.

What We Are Doing

Once we learned of the unauthorized access of the legacy server, we moved quickly to secure our systems and sensitive information. In addition to our own internal investigation, we retained a leading cybersecurity forensics firm and contacted law enforcement, and continue to work closely with them as they conduct their ongoing investigation. As it relates to the stolen laptop, the device is password protected and remote monitoring software has been set up to monitor for a connection to the stolen device, and should it occur, an automated attempt will be made to connect to the machine and erase its contents.

What You Can Do

While credit monitoring and identity protection services are not available for deceased individuals, there are steps you can take to request a copy of your deceased family member's credit report. An executor or surviving spouse can place a request to any of the three credit reporting agencies for a copy of the deceased individual's credit report along with making one of the following notations:

- "Deceased – Do not issue credit"; or
- "If an application is made for credit, please notify the following person(s): (e.g., list a surviving relative, executor/trustee of the estate and/or local law enforcement agency – specifying the relationship)."

Contact information for the three national credit reporting agencies for the purpose of requesting credit reports or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on credit files, is as follows:

Equifax
1-800-349-9960
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-888-909-8872
www.transunion.com
P.O. Box 2000
Chester, PA 19022

For more information regarding identity theft and the deceased, please visit <http://www.idtheftcenter.org> and search for "FS 117 - Identity Theft and the Deceased - Prevention and Victim Tips." You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You should also notify the Social Security Administration and the Internal Revenue Service of the death of your family member and that you received this letter.

This notice has not been postponed at the request of a law enforcement agency; however, we did communicate with law enforcement prior to issuing this notice.

Iowa Residents: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
and on-line at <http://www.iowaattorneygeneral.gov>

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft at:

Office of the Attorney General
220 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.com

Rhode Island Residents: We believe that this incident affected nine Rhode Island residents.

You can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400

Other
Important
Information

For More
Information

We apologize for any inconvenience or concern that these incidents might cause you. Should you have any questions, please feel free to call Todd Adams at 1-866-495-7322 between 9:00 a.m. and 5:00 p.m., Eastern time, Monday through Friday.