



February 22, 2016

Dear Mercy Housing Colleagues and former Mercy Housing Colleagues,

As those of you we were able to reach by email know, late Friday afternoon there was an unauthorized release of an electronic copy of all 2015 W2s issued by Mercy Housing's payroll department due to an email scam. As a result, unauthorized individuals may have personal information about you. This is a security breach of personal information.

We have contracted with two organizations to support you at this time. Their services are available for all current and former employees. We encourage you to complete the following steps as soon as possible:

Credit Monitoring - We have contracted with a credit monitoring agency, LifeLock, to provide you with free credit monitoring for 3 years. We suggest you enroll with LifeLock as soon as possible. To enroll go to: <https://store.lifelock.com/enrollment>

YOU HAVE UNTIL APRIL 30, 2016 TO REGISTER. When you go to enroll you should enter MHM16 in the box on the enrollment page of LifeLock's website that asks for a **partner/promo code**. On the next page you should enter your last name and the last four numbers of your Social Security Number in the box that asks for **membership ID**. If you have any trouble registering please email: identitytheft@mercyhousing.org

Identity Theft Assistance – SupportLinc, Mercy Housing's EAP offers identity theft assistance to help you recover from, and minimize the impact of, a breach of your identity. The service includes a 30-minute phone consultation with an identity recovery professional. To contact them, please call 1-888-881-5462. Username: Mercy; Password: linc123.

If your identity has been compromised –

1. Notify the Federal Trade Commission either by visiting <http://www.identitytheft.gov> or calling them at 1.877.438.4338.
2. Notify Mercy Housing by emailing us at identitytheft@mercyhousing.org. By alerting us to your concern, we can notify federal agencies to support their investigation into this breach.

This letter includes a series of attachments which you will find helpful:

Attachment 1: A formal notice, similar to the one we sent out via email on Saturday, February 20.

Attachment 2: A flyer from SupportLinc with more details about their identity theft assistance.

Attachment 3: An information sheet about how to identify email and other online scams.

We are taking this situation very seriously. As soon as we were informed of the breach, we took immediate action to prevent a repeat of this violation and we have informed law enforcement and Federal agencies of this incident.

Finally, we want to say how much we regret this incident and you have our sincere apologies. Please do act on the recommendations in the notice and reach out to your Supervisor with questions or concerns.



Jane Graf
President and CEO
Mercy Housing



Michele Mamet
Chief Administration Officer
Mercy Housing



MERCY HOUSING INC.

2/22/2016

NOTICE OF DATA BREACH

WHAT HAPPENED:

Late in the afternoon of Friday February 19, 2016 there was an unauthorized release of an electronic copy of all 2015 W2s issued by Mercy Housing's payroll department due to an email scam. As a result, unauthorized individuals may have personal information about you. This is a security breach of personal information.

WHAT INFORMATION WAS RELEASED:

All 2015 W2s

The following personal information is included in the scanned documents:

- Your name,
- Address,
- Social Security number,
- Wage details and
- Tax withholdings.

WHAT ARE WE DOING ABOUT IT:

We are taking this situation very seriously. As soon as we were informed of the breach we took immediate action to prevent a repeat of the violation. We have informed law enforcement and Federal agencies of this incident. We did not delay notifying you because of their involvement.

In addition, to help protect you from the possibility of any potential identity theft we are going to be partnering with **LifeLock, Inc** a company that specializes in proactively preventing identity theft. Enclosed is information on how to activate this service. It is available for all employees and former employees, free of charge, for three years.

WHAT CAN YOU DO:

With the theft of W2 information, your 2015 tax filing may be impacted. ***We strongly recommend you visit the IRS website:***

<https://www.irs.gov/Individuals/Data-Breach-Information-for-Taxpayers>

Please review their advice and act accordingly

We also strongly suggest you contact the major credit reporting agencies to discuss additional steps you can take to prevent the use of your personal information, such as placing a "security alert" or a "security freeze" on your credit report. For your information, the following are the addresses and toll-free numbers for the three major credit reporting agencies. (DO NOT AGREE TO PAY A FEE FOR THIS)

Experian: (888) 397-3742
P.O. Box 9530
Allen, TX 75013
www.experian.com

Equifax: (800) 685-1111 or (888) 873-5392
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

TransUnion: (800) 680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

You can also notify the Federal Trade Commission using the header – FTC 303-850-2700

Via their website at:

<https://www.ftccomplaintassistant.gov>

Or by mail to

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Or by phone: 1-877-438-4338

You can obtain information from these sources about fraud alerts and security freezes.

OTHER IMPORTANT INFORMATION:

You will also receive

- Information about the credit monitoring service Mercy Housing will pay for;
- Names of contact people inside Mercy Housing to answer questions you may have;
- Instructions and contact details for additional agencies outside Mercy Housing you may want to contact to protect your identity; and
- Information about how to identify email scams.

FOR MORE INFORMATION CONTACT:

If you have general questions or if you believe your identity has been compromised please contact:

Janel Moseley - Benefits Administrator

identitytheft@MercyHousing.org

p: 303.830.3428

If you have questions about IT, email or other technology please contact

Chad Leverenz - Vice President, IT Infrastructure & Development

Cleverenz@mercyhousing.org

p: 303.830.3407

Jane Graf
President and CEO
Mercy Housing

Michele Mamet
Chief Administration Officer
Mercy Housing



"I'm glad that's behind me! Somebody had opened a credit card in my name to purchase pharmaceuticals online! That wasn't me!! But what was I to tell the credit companies? That's when I called SupportLinc. Straightening all that out myself – I'd still be at it."

identity theft assistance

SupportLinc's ID Recovery is a telephonic consultation service to help you recover from, and minimize the impact of, a breach of your identity.

- The program provides a free 30-minute consultation with an identity recovery professional, who will create a personalized action plan for you.
- Reduced time spent repairing compromised credit history.
- Restores peace-of-mind, while helping undo damage.
- Ongoing guidance as often as needed.

Support for everyday issues. Every day.

**1-888-881-LINC (5462)
www.supportlinc.com**

**Username: mercy
Password: linc123**

SUPPORT  LINC
EMPLOYEE ASSISTANCE PROGRAMS

What is a social engineering fraud?

Whether you call it a “scam”, “social engineering”, “email fraud”, they all mean the intentional deception for personal gain or to damage another individual. In social engineering fraud, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.

What is phishing?

Phishing is a form of social engineering. Phishing use email or malicious websites to solicit personal information by posing as a trustworthy organization or individual. For example, an attacker may send email seemingly from a reputable executive, credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Examples of phishing scams (via phone or email) include:

- Someone poses as a boss of a company instructing staff to make a wire transfer into the fraudster's account
- Fraudsters pose as the IT services department of a bank saying they want to make a test transfer- but it's not a test
- Fraudsters claim to be a supplier and ask for outstanding invoices to be paid into a new bank account
- Employees click on links within phishing emails containing malware which authorizes many small payments into the fraudster's account

What can you do?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- If you are unsure whether an email request is legitimate, talk to your Supervisor and call Information Technology.

If you have any questions about this, please call the Mercy Housing Help Desk at 303.830.3376 or email identitytheft@mercyhousing.org.