TERMINIX®

Office of the New Hampshire Attorney General
Asst. Attorney General in Charge
Department of Justice
Consumer Protection
33 Capitol St
Concord, NH 03301

Subject: Data Breach Notice

I'm writing today to inform your office of a recent data breach at Terminix and our former affiliate, ServiceMaster. This breach was caused by an employee responding to a credentials phishing email, allowing the criminals to access her email account in the cloud and setup a rule to forward emails to an account they setup, unbeknownst to the employee. Emails were forwarded from September 10th until September 22nd. As we reviewed the compromised emails, we discovered (on September 26th) one email contained an attached file which included the name, social security number, date of birth, employment dates, and the 401K provider's name as well as account balance. A total of 14,708 individuals (current and former employees of either Terminix or ServiceMaster), 61 who we believe are residents of New Hampshire, based on the contact information in our systems.

I've attached the notice that we emailed to the majority of affected individuals on October 9th. As an additional measure, we've also engaged a company (ID Experts / IDX) to assist us with communicating via letter, as well. It is the same notice provided via email (attached) and will be sent out on Monday. We've also engaged this company to offer two years of identity theft protection services, as described in the notice of breach, at no cost to the affected individuals.

If you have any questions or concerns, please use the information below to contact me directly.

Thank you,

Brooke Stapleton
Compliance Director
150 Peabody Place | L/E – 0085 | Memphis, TN 38103
M: +1 901 896 6046
E: brooke.stapleton@servicemaster.com

ServiceMaster

TERMINIX

NOTICE OF DATA BREACH

Terminix and our former affiliate, ServiceMaster, take the privacy and security of your personal information very seriously, and we strive to maintain transparency in how we handle your data. It is for this reason we are reaching out today.

What Happened?
On September 16th, the company discovered that a teammate had responded to a phishing scam, which allowed hackers to gain access to the teammate's Office 365 account and cause the teammate's emails to be auto-forwarded from the teammate's inbox to an external email account controlled by the hackers. The auto-forwarding began on September 10th and continued until September 22nd. Please note that this breach involved a hack into Office 365 at the cloud level and there was no malware or malicious software that infected the company's internal systems.

What Information was Involved?
Our review of compromised emails revealed that one email included a file which contained the name, social security number, date of birth, employment dates, 401K balance and the name of our 401K provider for 14,708 current and former teammates across the United States. Due to the sensitive nature of this information, it is possible that thieves can use it for identity theft. We do not know if the information has been used at this time. We are sending this notice to both Terminix and ServiceMaster teammates because these events took place before the completion of the sale of ServiceMaster brands, when everyone receiving this notice was employed under the ServiceMaster Global Holdings brand.

What We are Doing:
We have taken and continue to take a number of actions in response to the breach. We have disabled the forwarding of the emails and contained the breach. We modified our email filtering and account authorization protocol to help prevent similar data breach incidents. We are communicating to our teammates to be sure everyone is especially diligent regarding any potential scams as we continue to fight the battle with these criminals from repeated phishing attacks. We are requiring teammates to complete the annual security awareness training, and we have issued specialized training to particularly high-risk groups to help them recognize extremely sophisticated phishing attempts. We are working with law enforcement agencies to investigate this cybercrime and are notifying state authorities as well. We've notified the provider of our 401K plans and the major credit agencies. We are continuing to monitor the security of our systems and reinforce messages related to the importance of abiding by proper security and data handling measures.

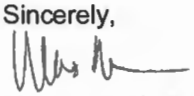
What you can Do:
While we currently have no reason to believe any personal information has been misused, for your protection, we have arranged to provide identity theft protection services through ID Experts®, the data breach and recovery services expert at no cost to you for two years. MyIDCare services include two years of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling toll-free at 1-833-752-0857 or going to https://app.myidcare.com/account-creation/protect and use the enrollment code shown below. **MyIDCare experts are available Monday through Friday from 9am – 9pm Eastern time. Please note that enrollment in MyIDCare services will be available starting October 13, 2021. Please do not attempt to enroll or contact ID Expert's call center before that time.** ***The deadline to enroll is January 11th, 2021.***

ENROLLMENT CODE: **[redacted]**

More Information
Additionally, we have enclosed information on steps you can take to further protect your information, and how to receive free credit monitoring. We take this matter very seriously and deeply regret any inconvenience or concern that this matter may cause you. If we need to update you on any new information related to this issue, you can find that posted on https://ide.myidcare.com/tmxsmb.

Sincerely,



Marcus A. McDaniel
Chief Ethics & Compliance Officer

MyIDCare

Recommended Steps to Help Protect your Information

1. Website and Enrollment. Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare (toll-free) at 1-833-752-0857 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina) or 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.