Attachment 1: Email sent to Designated Residential Customers

Subject: Important Notice About Your Personal Information

Hello [FirstName],

We want to let you know about an incident impacting your customer record.

- **What Happened:** ADT's cybersecurity systems detected unauthorized access to a limited set of customer and prospective customer data on April 20.
- **What We've Done:** We activated our response protocols immediately — terminating the intrusion, launching a forensic investigation with leading third-party cybersecurity experts, and notifying law enforcement.
- **What Information Was Involved:** The information involved was limited to names, phone numbers, and addresses. In a small percentage of cases, dates of birth and the last four digits of Social Security numbers were included.
- **What Was NOT Accessed:** No credit card or banking information was accessed, and if you are a current ADT customer, your security system is safe and was not accessed.
- **What We Are Offering:** In the coming weeks, we will offer complimentary identity protection services, as appropriate.

Protecting your privacy, ensuring transparency, and maintaining your trust are extremely important to us. As soon as we identified this issue, we acted quickly to contain it and launched a comprehensive investigation. The information accessed was limited to customer or prospective customer records and did not include any access to or impact on customers' security systems. Based on our investigation to date, we believe the unauthorized access was limited to related to you such as your name, address, phone number, date of birth, and the last four digits of your Social Security number, and did not include payment information such as bank accounts or credit card details.

Protecting customers' information is essential to ADT's mission, and the cybersecurity program remains an important and critical focus for the company.

For more information and updates on identity protection services, visit: adt.com/legal/security-notice.

Sincerely,
ADT

Attachment 2: Email sent to Designated Small Business Customers

Subject: Important Notice About Your Personal Information

Hello,

We want to let you know about an incident impacting your personal record.

- **What Happened:** ADT's cybersecurity systems detected unauthorized access to a limited set of customer and prospective customer data on April 20.
- **What We've Done:** We activated our response protocols immediately — terminating the intrusion, launching a forensic investigation with leading third-party cybersecurity experts, and notifying law enforcement.
- **What Information Was Involved:** The information involved was limited to names, phone numbers, and addresses. In a small percentage of cases, dates of birth and the last four digits of Social Security numbers or Tax ID were included.
- **What Was NOT Accessed:** No credit card or banking information was accessed, and if you are a current ADT customer, your security system is safe and was not accessed.
- **What We Are Offering:** In the coming weeks, we will offer complimentary identity protection services, as appropriate.

Protecting customers' information is essential to ADT's mission, and the cybersecurity program remains an important and critical focus for the company.

For more information and updates on identity protection services, visit: adt.com/legal/security-notice.

Sincerely,
ADT

Attachment 3: Links to ADT Security Notice Page and 8-K Filing

- **ADT Security Notice:** https://adt.com/legal/security-notice
- **8-K Filing:** https://d18rn0p25nwr6d.cloudfront.net/CIK-0001703056/eb8645ea-ddea-4d52-8ebb-2d72eed935da.pdf

Attachment 4: Notice Letter

ADT
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[FIRST NAME] [LAST NAME]
[ADDRESS]
[CITY, STATE ZIP]

June 29, 2026

Notice of Data Breach

Hello [FIRST NAME],

Thank you for reading this letter in its entirety.
As we've previously shared, ADT's cybersecurity systems detected unauthorized access to a limited set of customer and prospective customer data on April 20, 2026. The following provides more details about the incident and your affected data.

- **What Information Was Involved:** The information involved was limited to names, phone numbers, and addresses. In a small percentage of cases, dates of birth and the last four digits of Social Security numbers were included. Some ADT business customers may have also had Tax ID exposure.
- **What Was NOT Accessed:** No credit card or banking information was accessed, and if you are a current ADT customer, your security system is safe and was not accessed.
- **What We've Done:** We activated our response protocols immediately - terminating the intrusion, launching a forensic investigation with leading third-party cybersecurity experts, and notifying law enforcement.

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you on the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?
To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted, please provide the following unique code to receive services **[UNIQUE CODE].**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and email account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

erian (888) 397-3742	**Equifax (800) 525-6285**	**TransUnion (800) 680-7289**
. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
n, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
w.experian.com	www.equifax.com	www.transunion.com

Should you wish to obtain a credit report and monitor it yourself:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at (877) 322-8228. (Hearing impaired consumers can access their TDD service at (877) 730-4204.
- **Upon receipt of your credit report,** we recommend you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Cyberscout. Enrollment in the credit monitoring services is required for fraud resolution services.

What if I'd like more information regarding identity theft protection?

You can obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: (877) 438-4338; TTY: (866) 653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Protecting customers' information is essential to ADT's mission, and the cybersecurity program remains an important and critical focus for the company. For the latest details regarding this incident, please visit www.adt.com/about-adt/legal/security-notice. We're here to help!

Sincerely,

ADT