What should you do if contacted about a potential Cardholder data compromise?

We want to help you understand the steps you need to take if you find yourself in this situation.

A Cardholder data compromise is a loss or theft of Cardholder data that can:

- Happen when a criminal steals data from your Cardholder Data Environment
- Occur even if you don't store Card numbers
- Be hard for you to detect

If we suspect a Cardholder data compromise, we'll attempt to notify you.

TIP

If you have questions about any notifications from American Express, contact Merchant Services or your Client Manager.

Tips to Avoid Phishing

If you hear from us, you'll need to...

1 RESPOND

to AXPDataSecurity@aexp.com with contact info for the person you chose to work with us.

2 REVIEW

Look for security gaps in your Cardholder Data Environment.

TIP

Follow PCI DSS Guidance and include any supporting systems and third parties in your review. We may provide additional guidance or support as we work with you.

3 REPORT

Send an update about any security gaps you find to AXPDataSecurity@aexp.com.

IMPORTANT

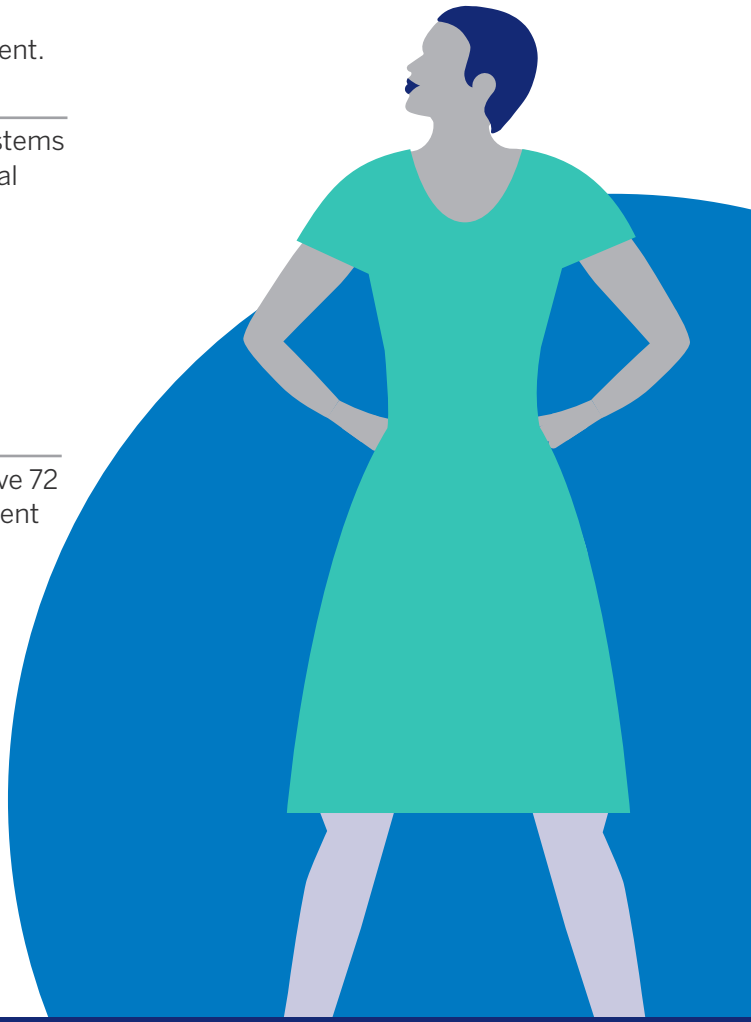
If you confirm a data incident has likely occurred, you have 72 hours from discovery to notify the Amex Enterprise Incident Response Program. Learn more

4 REMEDIATE

Fix the security gaps found during your review. Learn more about keeping payment data safe with the PCI Data Security Standard.

5 VALIDATE

Provide us with updated PCI DSS validation documents, as explained in Section 5 of our Data Security Operating Policy.



To learn more, visit **americanexpress.com/datasecurity**

AMERICAN EXPRESS

DON'T *do business* WITHOUT IT™