AMERICAN EXPRESS

Data Compromise Incident Report

Immediately contact the American Express Incident Response Program (EIRP) as soon as you suspect or confirm a data compromsie has occurred. Complete this form with known information and email it to eirp@aexp.com.

An incident manager will confirm receipt and will request additional details as required. The incident manager will also assist with the secure transfer of any sensitive information to American Express.

Important: Please review and adhere to the Data Incident Management Obligations as outlined in the American Express Data Security Operating Policy (DSOP) located at americanexpress.com/datasecurity.

Contact EIRP: eirp@aexp.com USA 1-888-732-3750 International +1-602-537-3021

Incident Reported By			
Name:		Email:	
Phone:		Company / Title:	
Impacted Entity			
Legal Entity Name:			
DBA Entity Name:			
Entity Address:			
City:		State / Province:	
Postal / Zip Code:		Country:	
Website URL(s):			
Amex Account Identifiers: (e.g. MID, Merchant ID, SE#)			
Type of Entity: (e.g. merchant, third party service provider)			
Payment Methods Accepted: (e.g. POS, online, phone / mail order)			
Corporate or Franchise Owned? (include # of locations)			
Impacted Entity Primary Contact			
Name:		Email:	
Phone:		Title:	
Impacted Entity Acquirer, Processor, and/or OptBlue Partner Contact (if applicable, e.g. Fiserv, PayPal, Stripe)			
List Acquirer, Processor, and/or OptBlue Partner(s) and their Contact Info (incl. Name, Email, and Phone):			

Incident Details

Please provide all known details. If a PCI Forensic Investigator (PFI) has been contracted to perform a PFI investigation, many of the questions below will be answered in the PFI's final investigation report.

Summary: Provide a description of the incident (who, what, when, where, why, & how) including key dates and details. If the incident involves multiple locations or entities, attach a list including location name, address, and acquirer / processor of entity impacted.

Investigation Scope: What environment is in scope of the investigation? (e.g. online / ecommerce, point-of-sale devices, email server, file storage / transfer)

Identification: What date and how was the incident first discovered?	
Date:	
How:	

Intrusion: What date did the compromise first occur, and how was unauthorized access obtained?	
Date:	
How:	

Data Exposure Window: What is the period of data exposure? (i.e. date range data is considered at-risk)			
Start Date:		End Date:	

Data Exposed: List all data elements exposed (e.g. card number, expiration date, CID / CVV2, cardholder name, address, email, etc.)

Data Access / Acquisition: Is there evidence to suggest an unauthorized party accessed, viewed, exfiltrated, and/or otherwise obtained access to the data? If yes, explain.

Data Controls: Is there evidence to suggest any data available to the unauthorized party is not at-risk of exposure? If yes, explain. (e.g. data available to unauthorized party was encrypted, tokenized, masked)

Containment: Has the incident been contained / stopped? (i.e. data no longer at-risk of exposure)			
Contained (yes/no)?		Date Contained:	
By Whom / How?			

Remediation: What additional steps have you taken to remediate your environment, strengthen your security posture, and prevent recurrence? Provide details including dates.
Fraud / CPP: Have you received complaints of fraudulent transactions and/or a Common Point of Purchase (CPP)? If yes, provide details including dates.
American Express Impact: Please work with your Acquirer and/or Processor to provide a list of American Express 15-digit card account numbers that are considered at-risk and/or transacted during the data exposure window above. Attach a file to your response, preferably a text file with each account number listed on a separate row and send your response with encryption. If you are unable to send the file encrypted, Amex can provide a method to transmit the file(s) securely upon request.

Comments:	
Independent Investigation	
Was a third party engaged to perform an independent investigation?	
Forensic Company Name:	
Was the forensic company contracted to perform a PCI Forensic Investigation (PFI), or non-PFI investigation?	
What date is the forensic investigation scheduled for completion?	
Notifications and Law Enforcement	
Customer Notifications: Did, or does the entity plan to, notify impacted data subjects (i.e. customers)? If yes, attach a copy of the notification letter template and confirm the date notifications were first sent.	
Customers Notified (yes/no)?	
Date of First Notification:	
Comments:	

Regulator / Authority Notifications (USA / International): Did, or does the entity plan to, notify any USA or International regulators / authorities (e.g. Massachusetts Attorney General, EU DPA's)? If yes, attach a copy of the notification letter template, provide a list of the regulators / authorities notified, and confirm the date each regulator / authority was notified.

Regulators / Authorities Notified? (yes/no)	
List of Regulators / Authorities notified and date of notification for each:	
Comments:	
Public / Media Notifications: Did, or does the entity plan to, notify the media or make any form of public announcement? If yes, attach a copy of each notice made.	
Public Notified (yes/no)?	
List of public notices made and date of notification for each: (e.g. website notice, press release)	
Comments:	
Law Enforcement: Has the entity contacted, or been contacted by, law enforcement regarding this incident? (e.g. FBI, USSS, Europol, local police / agency)	
Law Enforcement Aware? (yes/no)	
List law enforcement agency name, contact, and incident filing number:	
Comments:	