



MODEL DATA SECURITY BREACH NOTIFICATION FORM

Notice to the Delaware Attorney General

**Delaware Department of Justice
Consumer Protection Unit
820 N. French Street, 5th Floor
Wilmington, DE 19801
security.breach.notification@state.de.us**

The Consumer Protection Unit of the Delaware Department of Justice is making this Model Data Security Breach Notification Form available to provide assistance and guidance to businesses and other entities who are subject to Delaware's data breach notification law and are required to give notice of a data breach to the Attorney General under Title 6, § 12B-102(d) of the Delaware Code.

The Consumer Protection Unit will deem use of this Model Data Security Breach Notification Form to constitute appropriate written notice to the Attorney General that is required under Title 6, § 12B-102(d) of the Delaware Code. Other forms of written or electronic notice may be appropriate, but must provide the same information sought by this form.

Do not use this form to provide the notice to consumers and other affected persons required under Title 6, § 12B-102(a) of the Delaware Code. A model form for that purpose is available on the Consumer Protection Unit's security breach notification webpage:

<https://attorneygeneral.delaware.gov/fraud/cpu/securitybreachnotification>

PLEASE NOTE: The information disclosed on this form, or otherwise provided to the Department of Justice pursuant to Title 6, § 12B-102(d) of the Delaware Code, may constitute a public record subject to disclosure under Delaware's Freedom of Information Act (Title 29, Chapter 100) ("FOIA"). FOIA requires that the Department of Justice's records are public records (unless otherwise declared by FOIA or other law to be exempt from disclosure) and are subject to inspection and copying by any person upon a written request. A person providing notice of a security breach to the Department of Justice may request confidential treatment when it delivers the notice, by identifying the information for which confidential treatment is sought, representing in good faith that the information is not a "public record" as defined in FOIA, and briefly stating the reason(s) why. The Department of Justice will independently determine the validity of the request for confidential treatment.



SECURITY BREACH NOTIFICATION FORM

Delaware Department of Justice
Consumer Protection Unit
820 N. French Street
Wilmington, DE 19801
security.breach.notification@state.de.us

Type of Report

- Initial Breach Report
- Addendum to Previous Report

Entity That Owns or Licenses the Computerized Data Whose Security Was Breached

Name:						
Street Address:						
City:		State:		ZIP Code:		

Submitted By

Name:				Title:			
Firm (if different):							
Street Address:							
City:		State:		ZIP Code:			
Telephone:			Email:				
Relationship to Entity That Was Breached:							

Type of Organization

- | | | |
|---|--|---|
| <input type="checkbox"/> Charitable/Non-Profit | <input type="checkbox"/> Educational | <input type="checkbox"/> Financial Services |
| <input type="checkbox"/> Government – Delaware | <input type="checkbox"/> Government – Outside Delaware | <input type="checkbox"/> Healthcare |
| <input type="checkbox"/> Insurance | <input type="checkbox"/> Retail/Merchant | <input type="checkbox"/> Utility |
| <input type="checkbox"/> Other (please describe): _____ | | |

Type of Personal Information Involved in the Security Breach

Delaware resident's first name or first initial and last name, in combination with 1 or more of the following (mark all that apply):

- | | |
|---|--|
| <input type="checkbox"/> Social Security number | <input type="checkbox"/> Driver's license number |
| <input type="checkbox"/> Federal identification card number | <input type="checkbox"/> Passport number |
| <input type="checkbox"/> Individual taxpayer ID number | <input type="checkbox"/> Biometric data |
| <input type="checkbox"/> Deoxyribonucleic (DNA) profile | <input type="checkbox"/> Medical history |
| <input type="checkbox"/> Medical treatment by a healthcare professional | <input type="checkbox"/> Diagnosis of mental/physical condition by healthcare professional |
| <input type="checkbox"/> Health insurance policy number, subscriber ID number, or any other unique identifier used by health insurer to identify person | |
| <input type="checkbox"/> Account number, credit card account number, or debit card number, in combination with any required security code, access code, or password that would permit access to a financial account | |
| <input type="checkbox"/> Username or email address, in combination with password or security question and answer to access online account | |

Number of Persons Affected

Delaware Residents Only	
Total (including Delaware)	

Dates

Breach(es) Occurred (include start/end dates if known)	
Breach(es) Discovered	
Consumers Notified	

Form of Notice to Affected Persons*

- | | |
|-------------------------------------|--|
| <input type="checkbox"/> Written | <input type="checkbox"/> Telephonic |
| <input type="checkbox"/> Electronic | <input type="checkbox"/> Substitute Notice |

Was Notification Delayed Because of Law Enforcement Request?

- Yes No

* Please attach a sample of the notice

Type of Security Breach (mark all that apply)

- | | | |
|--|--|---|
| <input type="checkbox"/> Loss or theft of device or media | <input type="checkbox"/> Internal system breach | <input type="checkbox"/> Insider wrongdoing |
| <input type="checkbox"/> External breach (<i>hacking, malware, etc.</i>) | <input type="checkbox"/> Payment card fraud | <input type="checkbox"/> Inadvertent disclosure |
| <input type="checkbox"/> Improper disposal | <input type="checkbox"/> Other (<i>please describe</i>): _____ | |

Was Information Encrypted?

- Yes No

Was Encryption Key Acquired?

- Yes No N/A

Brief Description of the Security Breach

Location of Breached Information

- | | | |
|--|---|-------------------------------------|
| <input type="checkbox"/> Desktop computer | <input type="checkbox"/> Portable/Laptop computer | <input type="checkbox"/> Smartphone |
| <input type="checkbox"/> Network server | <input type="checkbox"/> Cloud-Based Server | <input type="checkbox"/> Email |
| <input type="checkbox"/> Other (<i>please describe</i>): _____ | | |

Actions Taken in Response to the Security Breach (mark all that apply)

- | | |
|--|--|
| <input type="checkbox"/> Added/strengthened data encryption | <input type="checkbox"/> Changed password/strengthened password requirements |
| <input type="checkbox"/> Created/updated formal written information security plan | <input type="checkbox"/> Implemented new technical safeguards |
| <input type="checkbox"/> Improved physical security | <input type="checkbox"/> Revised policies and procedures |
| <input type="checkbox"/> Sanctioned workforce members involved (incl. termination) | <input type="checkbox"/> Trained or retrained workforce members |
| <input type="checkbox"/> Implemented periodic technical and nontechnical evaluations/risk analyses/penetration tests | |
| <input type="checkbox"/> Revised contracts with business partners, vendors, subcontractors, service providers | |
| <input type="checkbox"/> Changed business partners, vendors, subcontractors, service providers | |
| <input type="checkbox"/> Other (<i>please describe</i>): _____ | |

Credit Monitoring or Identity Theft Protection Services Offered?

<input type="checkbox"/> Credit monitoring <input type="checkbox"/> Identity theft protection	Duration:	
	Provider:	
Briefly describe services:		

Law Enforcement Agency Notified of Security Breach?

<input type="radio"/> Yes <input type="radio"/> No	Name of Agency:	
	Contact Name and Number:	
	Report Number (<i>if applicable</i>):	