

NOTIFICATION OF SPECIFIC EVENTS

Notification

The District will notify the New York State Attorney General (AG), the New York State Department Consumer Protection Board (CPB) and the New York State Office of Cyber Security (OCS), as required by law. All affected individuals must be notified of the breach if their compromised data meets the classifications described in law. The District may delay notification of affected individuals if law enforcement determines that notification may impede a criminal investigation.

The required notice shall be directly provided to the affected persons by one of the following methods:

1. Written notice;
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the District when notifying affected persons in electronic form. However, in no case shall the District require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;
3. Telephone notification, provided that a log of each such notification is kept by the District when notifying affected persons by phone; or
4. Substitute notice, if the District demonstrates to the State Attorney General that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds \$500,000, or that the District does not have sufficient contact information. Substitute notice shall consist of all of the following:
 1. Email notice when the District has an email address for the subject persons;
 2. Conspicuous posting of the notice on the District's website page, if the District maintains one; and
 3. Notification to major statewide media.

Regardless of the method of which notice is provided, a notification must include:

1. Contact information for the District official handling the notification;
2. A description of the categories of information that were, or are reasonably believed to have been, acquired without authorization; and
3. Details on which elements of personal and private information were, or are reasonably believed to have been, so acquired.

The New York State Office of Cyber Security will be informed as to the timing, content and distribution of the notices and the approximate number of affected persons. The Attorney General and the Division of Consumer Protection should also be informed of these notices to affected

persons. Refer to Form #5672 -- New York State Security Breach Reporting Form for contact information, addresses and notification guidelines.