Crisis Communications Plan for Data Breach of Loyallist® Rewards Program

Drafted: November 4, 2021

Table of Contents

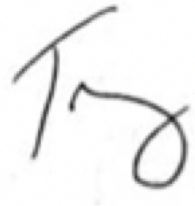
Introduction

Bloomingdale's makes fashion personal and fun, aspirational yet approachable. Our mission is to guide and inspire our customers to make style a source of creative energy in their lives. We will always strive to make Bloomingdale's like no other store in the world. To continue our role as America's premier designer shopping destination, we must exercise careful planning and proactive thinking to prevent any major disruptions or crisis situations within our organization.

In order to safeguard our organization against potential threats, we must take adequate precautions to prepare for an unforeseeable crisis scenario. With that in mind, the purpose of this crisis communications plan is to educate, organize, and prepare our organization in the case of a data breach targeting sensitive information of our customers enrolled in the Loyallist® rewards program. This plan provides a framework for crisis messaging and will help colleagues respond to the data breach or other cyber-attack incident effectively and promptly. Without proper planning, Bloomingdale's would suffer significant reputational and financial losses, as well as a severe impact on the overall customer experience.

While I hope we never experience a crisis of this nature, precautionary measures are invaluable. I encourage everyone to review the contents of this crisis plan to help facilitate a swift recovery in the case of a data breach. By understanding your role, you can help contain a potential crisis and maintain our status as the store like no other in the world for years to come.

With respect,



Tony Spring
Chairman and Chief Executive Officer
Bloomingdale's

Acknowledgements

The following members of Bloomingdale's executive leadership and applicable staff have read this crisis communications plan in its entirety and understand their role. By signing below, this crisis communications plan is considered to be endorsed, and all responsible colleagues will pledge support to the actions as they are outlined.

Executive Leadership

_____

Tony Spring, Chairman & CEO

_____

Charles Anderson, EVP & Director of Stores

_____

Keri Taub, Vice President of Strategy

Communications Team

_____

Kevin Harter, Vice President of Integrated Marketing

_____

Brigitte Timmins, Director of Earned Media

_____

Jennifer Whalen, Director of Internal Communications

_____

Sebastian Masmela, Sr. Manager of Media Relations

Rehearsal Dates

A successful implementation of this crisis communication plan requires routine rehearsal every 6-12 months. Full-scale rehearsals will be performed on an annual basis in March and will include a mock data breach scenario to test Bloomingdale's crisis response. Tabletop rehearsals, along with a crisis plan review, will also be conducted on an annual basis in September. While the rehearsal dates are subject to change at the discretion of senior leadership, the 2022 rehearsal schedule is attached below:

FULL-SCALE REHEARSAL + MOCK SCENARIO**.....** MARCH 15, 2022

TABLETOP DRILL + CRISIS PLAN REVIEW**.....** SEPTEMBER 20, 2022

Purpose and Objectives

Purpose Statement

In a crisis scenario where the privacy of our customers enrolled in the Loyallist® rewards program is compromised, Bloomingdale's will act with poise and professionalism using open and honest communication with all key publics. Our organization will put our customers first by disclosing information in a timely manner and creating open channels of communication between our organization and those that are connected to us.

Objectives

1. Maintain transparency and facilitate cooperation amongst all relevant publics, as listed in the crisis directory, the list of key media, and the list of organization spokespersons, by enforcing a three-hour notification period after the crisis is detected.
2. Improve the efficiency of Bloomingdale's communication platforms by executing clean, thoughtful communications that hit all key messages and ease the concerns of customers affected by the data breach.
3. Follow the guidelines set in the crisis communication plan closely so that the organization can handle the crisis quickly and appropriately, thus minimizing reputational damage and showcasing our values of dedication and preparation.
4. Highlight Bloomingdale's commitment to our customers and their experience by learning from the data breach and communicating to our publics that we will implement new and additional security measures to protect our customer's privacy.

Crisis Inventory

This crisis inventory for Bloomingdale's lists the types of events that a midsize, high-value department store with national presence of could be the target of, such as on-site incidents, including but not limited to: an active shooter or suicide, robbery, closure of stores or distribution centers, and layoffs, among other things. Additionally, the organization could be subject to cybercrimes such as data breaches, as well as corporate-level issues, like briberies, bankruptcy, and discrimination.

Charting these possible crises resulted in an inventory ranked by possibility and damage potential. The scale used for possibility ranks from 0 to 5, which is measured as follows:

0 = Impossible, no chance of occurring
1 = Nearly impossible
2 = Remotely possible
3 = Possible
4 = More than possible, has happened before to your organization or similar organizations
5 = Highly probable, warning signs are evident

The scale used for damage potential also ranks from 0 to 5, which is defined as follows:

0 = No damage nor serious consequences
1 = Little damage, can be handled without much difficulty
2 = Some damage, slight chance the media will be involved
3 = Considerable damage, impact on organization but not a major media/public event
4 = Considerable damage, definitely could be a major media/public event
5 = Devastating, front-page news and could seriously damage organization's reputation

Continue to the next page to view the charted crisis inventory.

Crisis	Possibility (0-5)	Damage (0-5)
Shooter/Suicide	2	4
Robbery	2	3
Store/Distribution Center Closure	3	3
Layoffs	2	2
Data breaches	4	4
Executive-level briberies	1	5
Bankruptcy	1	5
Workplace discrimination	2	4

Based on the rankings in the above inventory, the threat of a data breach merits its own distinct crisis communications plan, as it is the most likely crisis scenario with a high level of potential damage. Our competitors, Neiman Marcus, and Saks Fifth Avenue have also endured similar crises in recent years. Thus, it is imperative that we take the necessary steps to be prepared in the case of a crisis scenario as severe as this.

Key Publics

Enabling Publics

- Senior executives
- Shareholders

Functional Publics

- Customers
- Colleagues
- Unions (for unionized stores & distribution centers)

Normative Publics

- Competitors
- Trade associations

Diffused Publics

- Broadcast news media
- Print news media

Notifying Publics

The colleague who first detects the crisis will notify their supervisor and/or Vice President as soon as possible, who will then immediately notify the CEO via phone. The CEO is then responsible for activating the crisis communications plan by notifying the crisis team.

The crisis team will manage the process of notifying publics. The table below identifies the appropriate colleague and corresponding channels that will be used to notify each of the organization's key publics.

	Methods of Communication							
	Phone	**Email**	**Social Media**	**Mailed Letter**	**Website**	**In-Person Visit**	**News Release**	**Meeting**
Senior executives	Kevin	Kevin				Kevin		Kevin
Shareholders	Kevin	Kevin		Kevin		Kevin		Kevin
Colleagues		Jennifer						Jennifer
Internal IT Teams	Jennifer	Jennifer						Jennifer
Customers		Kevin	Brigitte		Kevin			
Unions	Jennifer	Jennifer						Jennifer
Competitors					Kevin			
Trade associations		Kevin			Kevin		Sebastian	
Broadcast news media	Brigitte	Brigitte	Brigitte		Brigitte		Sebastian	
Print news media	Brigitte	Brigitte	Brigitte		Brigitte		Sebastian	

Crisis Communications Team

***Crisis Manager*:** Kevin Harter, Vice President of Integrated Marketing
Responsibilities:

- Communicate with senior executives and lead all external communications.
- Approve final deliverables (e.g., digital content, news releases, statements) for external distribution.
- Make critical decisions during a crisis.
- Provide direction for other crisis team members.
- Update senior executives and communications team on crisis' progression.

Assistant Crisis Manager: Brigitte Timmins, Director of Earned Media
Responsibilities:

- Takes on responsibilities of the Crisis Manager when he is unavailable.
- Leads direction of key messaging and statements.
- Coordinates media inquiries and correspondence.

Control Room Coordinator: Jennifer Whalen, Director of Internal Communications
Responsibilities:

- Sets up the crisis communications control center.
- Ensures that the control center is stocked with all necessary equipment.
- Leads all internal communications initiatives.

Crisis Communication Colleague: Sebastian Masmela, Sr. Manager of Media Relations
Responsibilities:

- Assists with the notification of key stakeholders.
- Drafts news releases, external emails, social media content, and other deliverables for external audiences.
- Additional duties as assigned by the Assistant Crisis Manager.

Crisis Directory

The crisis directory contains the contact information for the crisis team and relevant senior executives.

Crisis Team			
Name	**Role**	**Phone**	**Email**
Kevin Harter	Crisis Manager		Kevin.Harter@bloomingdales.com
Brigitte Timmins	Assistant Crisis Manager		Brigitte.Timmins@bloomingdales.com
Jennifer Whalen	Control Room Coordinator		Jennifer.Whalen@bloomingdales.com
Sebastian Masmela	Crisis Communications Colleague		Sebastian.Masmela@bloomingdales.com

Relevant Senior Executives			
Name	**Title**	**Phone**	**Email**
Tony Spring	Chairman & CEO		Tony.Spring@bloomingdales.com
Charles Anderson	EVP & Director of Stores		Charles.Anderson@bloomingdales.com
Keri Taub	VP of Strategy		Keri.Taub@bloomingdales.com

Media Spokespeople

Primary Spokesperson: Tony Spring, Chairman & Chief Executive Officer

Secondary Spokesperson: Keri Taub, Vice President of Strategy

Cybersecurity Spokesperson: Andres Noriega, Senior Director of Information Technology

List of Emergency Personnel

This list below includes all emergency personnel on a local, state, and national level to be contacted as soon as the data breach is detected.

Emergency Contact Information		
Agency Name	**Phone**	**Address**
NYPD – Computer Crimes Squad	(646) 610-5000	153 East 67th Street New York, NY 10065
New York State Bureau of Criminal Investigation – Computer Crimes	(518) 474-5330	1220 Washington Avenue Bldg. 22 Albany, NY 12226
FBI – New York Bureau	(212) 384-1000	26 Federal Plaza, 23rd Floor New York, NY 10278
Federal Trade Commission – Northeast Region	(212) 607-2829	1 Bowling Green #318 New York, NY 10004

Key Media

Listed below are national media outlets based in New York. It is the responsibility of Sebastian Masmela, Crisis Communication Colleague, to update this list annually prior to the full-scale rehearsal exercise to ensure contact information is up to date.

Broadcast Outlets			
Outlet	Media Contact	Phone	Email
WABC-TV			
WNBC-TV			
WCBS-TV			
WNYW-TV (Fox)			

Print Outlets			
Outlet	Media Contact	Phone	Email
The New York Times			
Wall Street Journal			
USA Today			
Forbes			

Industry Outlets			
Outlet	Media Contact	Phone	Email
Business Insider			
CNBC			
CNET			
Compliance Week			

Crisis Communications Control Center

In the event of a data breach relating to the Loyallist® rewards program, Bloomingdale's LIC corporate office will remain unaffected. All crisis team colleagues will leave their individual workspaces (remote or in-person), and report to Conference Room 7 at the start of each workday. The LIC address is listed below:

Bloomingdale's LIC Corporate Office:
28-07 Jackson Avenue
Long Island City, NY 11101

Equipment and Supplies

Supplies:

- Clipboards
- Company letterhead
- Whiteboard and dry erase markers
- Printer paper
- Writing materials (pencils, pens, and lined paper)
- Bulletin board
- Coffee machine
- Bottled water
- Snacks
- Filing cabinet

Technology:

- Laptop computers and chargers
- Additional monitors
- HDMI cables
- Video production/lighting equipment
- Microphone/headphones for remote interviews
- iPhone tripod
- Secure VPN
- Prepaid wireless modem
- External hard drive
- Extension cords
- Printer and scanner

Media:

- Hardcopies of the crisis communications plan
- Media directories
- Press kits
- Loyallist® information sheet

Pre-Gathered Information

The pre-gathered materials listed below will be stored in a password-protected Microsoft OneDrive folder that is dedicated to this crisis communications plan. Additionally, each member of the crisis team and relevant senior executives will keep a copy of the following documents in an encrypted flash drive at a private, secure location of their choosing. Each person is responsible for updating the documents from Microsoft OneDrive on a monthly basis to ensure all materials are current.

Hard copies of the following documents should also be kept with the flash drive to ensure all relevant colleagues have easy access to the crisis communications plan. These hard copies should also be updated monthly from Microsoft OneDrive to ensure each colleague has the most updated version of the documents.

- Biographies of senior executives and crisis team colleagues
- Copies of the crisis communications plan
- Financial information from the past two years
- Loyallist® backgrounders and brochures
- Skeletal news release about Loyallist® data breach
- Most recent FAQ documents
- Documentation that lists cybersecurity updates, recent trainings, and current systems

Key Messages

General Key Messages

- Bloomingdale's has been providing customers with luxurious shopping experiences for over 125 years.
- Bloomingdale's is America's only nationwide, full-line, upscale department store.
- Bloomingdale's mission is to make fashion a creative source in people's lives by making it fun and personal, and aspirational yet approachable.

Crisis-Specific Key Messages

- A data breach affecting customers that are part of Bloomingdale's Loyallist® rewards program was detected at [TIME] on [DATE]. All applicable customers have been notified of this data breach.
- The breach came in the form of a malware attack, with our systems being hacked from an external, remote source. Bloomingdale's IT team was notified within [TIME] of detection.
- As of [TIME] on [DATE], this data breach has potentially impacted [NUMBER] customers. Non-participants in the Loyallist® rewards program are not impacted by this data breach, and their information remains secure.
- To safeguard the information of the Bloomingdale's community, our IT team is actively [SECURITY MEASURES TEAM IS TAKING].
- Our IT team is working diligently with [AUTHORITIES] to find the identity of the hacker. Bloomingdale's is currently operating in-store and online shopping experiences normally.
- For the latest information regarding the data breach, visit the cybersecurity banner on our website: [LINK TO NEW WEBSITE PAGE].

Bloomingdale's
28-07 Jackson Avenue
Long Island City, NY 11101
(800) 777-0000

FOR IMMEDIATE RELEASE

BLOOMINGDALE'S TARGETED IN DATA BREACH OF LOYALTY PROGRAM

NEW YORK – National high-end retailer Bloomingdale's was targeted in a cybersecurity attack on [DATE] at [TIME]. This breach of the Loyallist® rewards program came in the form of a malware attack from an external, remote hacker.

The attack was first detected by a Bloomingdale's colleague, who notified the IT team within [TIME]. All affected customers were notified immediately following detection. As of [TIME] on [DATE], this data breach has potentially impacted [NUMBER] customers. Non-participants in the Loyallist® rewards program are not impacted by this data breach, and their information remains secure.

"Our Loyallist members are a crucial part of the Bloomingdale's community, and we are deeply concerned with the privacy violations this cyberattack has caused," said Tony Spring, chairman & CEO. "We are working diligently with [AUTHORITIES] to identify the hacker and ensure this does not happen again."

To safeguard customer information, Bloomingdale's is actively [SECURITY MEASURES TEAM IS TAKING].

In-person and online shopping experiences at Bloomingdale's are currently operating normally. For more information about the data breach, and to learn about new corrective measures, please visit the cybersecurity banner online at: [LINK TO NEW WEBSITE PAGE].

###

Media Contact: Brigitte Timmins, Brigitte.Timmins@bloomingdales.com, (212) 417-1928

About Bloomingdale's
Bloomingdale's is America's only nationwide, full-line, upscale department store. It was founded in 1872 and currently operates 33 Bloomingdale's stores and 21 Bloomingdale's, The Outlet Stores, in 14 states, along with 1 Bloomie's location in Virginia. In addition, Bloomingdale's has an international presence with a location in Dubai. Be sure to follow @bloomingdales on social media, become a Loyallist, and for more information, or to shop any time, visit www.bloomingdales.com.

Website

Kevin Harter, Crisis Manager is responsible for approving updates to the website. The website will feature a unique "cybersecurity" banner at the top of all pages on the website dedicated to information about the data breach and will be live within 24 hours of detection.

Statement from Bloomingdale's Leadership
In the event of a crisis where a data breach impacts customers that are part of Bloomingdale's Loyallist® rewards program, Kevin will update the website with a statement coming from Chairman & CEO Tony Spring expressing concern about the data breach and explain the proactive measures Bloomingdale's is taking to prevent future attacks. This will appear at the top of the page that the cybersecurity banner redirects to.

Crisis Information
In addition to the statement from the chairman & CEO, Bloomingdale's will include all press releases and media updates on the new website page for the duration of the crisis. These updates will be posted at the same time they are released to the press, in order to achieve transparent and timely communication best practices and to rebuild trust with the public.

Cybersecurity Resources
Bloomingdale's will provide an extensive list of resources for customers impacted by the data breach to demonstrate that the organization is committed to protecting their privacy. Additionally, this section will include a list of resources that customers can reach out to if they have further questions or concerns about their exposure.

Preventative Policies and Other Documentation
Bloomingdale's preventative policies and latest systematic software updates will be listed on the webpage to show what precautionary measures have already been taken to prevent such a crisis. After the crisis has been effectively dealt with, and the crisis team has gathered results of the evaluation, Bloomingdale's will provide a statement on how it will update its standard operating procedures and augment its cyber policies to mitigate future crises of this nature.

Blogs and Social Media

Brigitte Timmins, Assistant Crisis Manager, is responsible for posting frequent and transparent on Bloomingdale's social pages. This includes the organization's pages on Facebook, Instagram, Twitter, and LinkedIn. Additionally, Brigitte and Sebastian are responsible for monitoring the aforementioned social media sites, blogs, online outlets, print outlets, and broadcast outlets for coverage relating to the data breach.

Updates to Social Media Accounts
All updates posted on social media platforms will maintain a professional and apologetic tone, and direct audiences to the same page as the "cybersecurity" banner on the Bloomingdale's website. Additionally, all updates to the press will be accompanied with social media posts to allow for an equal flow of information. During this time, posts will stress that in-person and online shopping experiences are operating normally.

Brigitte and/or Sebastian will respond to all messages authentically and respectfully within ten (10) minutes. They will closely follow the practices outlined in the organization's social media user policy. They will also respond to questions being asked by users in the "Comments" section of posts.

Media Monitoring
Brigitte and Sebastian will be responsible for monitoring relevant coverage on social media platforms and news outlets at the beginning and end of the business day, as well as at noon ET. Bloomingdale's will closely monitor the tone of online conversation about the crisis and update its messaging accordingly to reassure and inform its publics. The following monitoring practices will be used:

- *Social media platforms:* Brigitte and Sebastian will monitor the aforementioned social media platforms using Hootsuite. They will search using the following keywords: "Bloomingdales" OR "Bloomies" OR "Loyallist" AND "data breach" OR "attack" OR "cyber" OR "scam" OR "security" OR "privacy"
- *Broadcast outlets:* Sebastian will use Critical Mention and input the same keywords as above.
- *Online outlets and blogs:* Brigitte will use Google Alerts with the following keywords: "Bloomingdales" AND "data" OR "cyber"
- *Print outlets:* Sebastian will use Google Alerts with the same keywords as above, looking especially for stories that will also be featured in print editions.

Trick Questions

Q: If Bloomingdale's had more advanced cybersecurity firewalls in place to protect the privacy of its reward program members, could this attack have been prevented?
A: It is unrealistic to speculate the difference other cybersecurity measures could have made in this data breach.

Q: How are customers expected to trust Bloomingdale's with sensitive information if their privacy has been exposed?
A: Bloomingdale's deeply values our Loyallist rewards members for trusting us with their needs and providing vital information to offer them an elevated client experience both in-person and online. We understand that their privacy and security is of the utmost importance, and we hope that by updating our software and amending our cybersecurity practices, they can rest assured that we are taking necessary precautions to prevent another data breach.

Q: Do you suspect that this attack was conducted by a disgruntled employee or someone else in the Bloomingdale's community?
A: While we know the data breach was conducted from an external, remote location, we cannot speculate the identity of who is responsible. We are working closely with [AUTHORITIES] to investigate the source of the data breach and will release a comprehensive report once the investigation has concluded.

Q: Were there any warning signs that a data breach like this was likely to occur?
A: Bloomingdale's takes warning signs very seriously and tracks potential threats that could be considered dangerous to our organization and community…
-If YES: The following cybersecurity concerns were presented to management during the past year: [LIST OF CONCERNS]. After being notified, we took the necessary steps to remedy the situation and update our programs and procedures to prevent future problems.
-If NO: During the past year, there were no reported concerns relating to cybersecurity and data integrity.

Q: How often does Bloomingdale's update its cybersecurity software and procedures?
A: Bloomingdale's conducts periodic maintenance checks every [TIME INTERVAL]. We also work closely with our Information Technology colleagues to ensure our systems are up to date and functioning properly.

List of Prodromes

Warning signs indicating a potential data breach of the Loyallist® rewards program include:

- Outdated cybersecurity software
- Policy violations relating to cybersecurity and data integrity
- Using the same database passwords for more than three (3) months
- Frequent usage of unsecured Wi-Fi networks by colleagues
- Loss of colleague-assigned equipment (e.g., company-owned laptops and cell phones)

Evaluation Form

The following evaluation should be completed by all who participated in the crisis response effort. At a minimum, this form is mandatory for the crisis team, and relevant senior executives.

Name and Date: _____

Date and Time of Crisis Detection: _____

Most Recent Crisis Rehearsal Date: _____

Person/Department That Detected Crisis: _____

Time Until Crisis Team Activation: _____

How much time elapsed between crisis activation and notification of the key publics? The media?

_____

Were you able to easily locate a copy of the crisis communications plan? Yes No

Was the crisis communications plan followed? Yes No

Was there any information missing from the crisis communications plan? Yes No

-If yes, please list what information would've been helpful: _____

_____

What aspects of the crisis communications plan were executed well? Executed poorly?

_____

_____

_____

What could the crisis team do differently during the next crisis to help lessen its severity or its impact on Bloomingdale's reputation?

_____

_____

_____

_____