VIRTUAL CONFERENCE

ACFE GLOBAL
FRAUD CONFERENCE
JUNE 22–24, 2020 | ONLINE VIRTUAL CONFERENCE

ACFE®
Association of Certified Fraud Examiners

Multi-Dimensional Cyber Communications: It's More Than Notification and Compliance

Jack Healey, CFE, CPA/CFF, CRISC
Chief Executive Officer
Bear Hill Advisory Group

LIGHT the WAY

A beacon of light in uncertain times.™

Multi-Dimensional Cyber Communications: It’s More Than Notification and Compliance

ACFE GLOBAL
FRAUD CONFERENCE
June 22-24, 2020 | Virtual Conference

It’s not what you say, but what you don’t say

BEAR HILL
ADVISORY GROUP

Our Speaker Today

- Bear Hill Advisory Group helps companies turn business risks into value
- Through our business rescue services we help companies be prepared for and overcome their worst days
- Cybersecurity incidents, ethical and integrity breaches, fraud, embezzlement, product recall, Foreign Corrupt Practices Act, and serious fraud violations

Jack P. Healey, CFE, CPA/CFF, CRISC
Chief Executive Officer, Bear Hill Advisory Group, LLC

Jack is an expert in operational, financial and organizational crisis management, strategies, and tactics. He is an expert in cyber incident response strategies and tactics.

He is a Certified Fraud Examiner, Certified Public Accountant, Certified in Fraud and Forensics, Cybersecurity SOC, and Cybersecurity Services. He is a member of ACFE, InfraGard, ISACA , AICPA, and NACD.

He authored the Business Crisis Diagnostic and Prevention Model™, which provides businesses with the framework necessary to identify impending business crises before they occur.

AGENDA

- What are the dimensions of a multi-dimension communication plan?
- The role of the three Cs
- Message maps—What they are and how to construct them
- How do you choose how to communicate?
- Sample message maps

Quote 1

"There cannot be a crisis next week. My calendar is already full."

Henry Kissinger,

Former U.S. Secretary of State

50 Breaches First Quarter 2020

BEAR HILL
ADVISORY GROUP

Company	Booty	# Records
Landry's	Credit Card data	Unknown
Alomere Health	Health Care Data	49,351
Amazon Web Services	British Passports	Unknown
PlanetsDrugDirect	Pharmacy	Unknown
Mitsubishi Electric Corp	Gov Exchange Info	Unknown
Greenville water	Payment Info	500,000
SexPanther	Bio Metrics, PII	11,000
The Royal Yachting Assoc	Members Database	Unknown
Oman United Ins Company	Ransomware	Unknown
Florida Library	Staff Computers	600
Marriott	PII of guests	52,000,000
Munson Healthcare	PII + PHI	Unknown
Microsoft	Support logs 250 customers	Unknown
Perth Mint	Questionnaire Data	1,480
Social Captain	Co's source code	Unknown
Yarra Trams	Personal Emails	Unknown
Bouygues Construction	Ransomware 200GB of data	Unknown
Fondren Orthopedic	PII + PHI	30,049
St Louis Community College	PII	5,127
Jokers Stash	CC including CVV/CVC	461,876
Israeli Netanyahu's Party	Israel's entire voting registration	65,000,000
Enrichment Systems Inc	PII + PHI	Unknown
Estee Lauder Companies	PII	440,000,000

Rutter's Convenience Store	Credit card CVV	Unknown
South-central Iowa Medical system	PII	7,500
MGM Resorts	PII	10,600,000
Minister of Education	Educators PII	360,000
Decathlon	Customer and Employee Data	123,000,000
Britain's Financial Conduct Authority	List of complainants	Unknown
Slickwraps	PII	850,000
Transavia	PII and need for physical assistance	80,000
Company Clearview AI	AI Facial Recognition	3,000,000,000
Lincoln County	Employee PII	Unknown
Railworks Corp	PII former employees	Unknown
Straffic	Customers data	49,000,000
Walgreens	PII- Prescript #	Unknown
UK Railway Stations	ID for free wi-fi	10,000
J Crew	Last 4 digits cc, email and shipping	Unknown
J Crew	passwords cell phone numbers	266,000
Princess Cruises and Holland America Line	PII including passport Infor	Unknown
T-Mobile	PII	Unknown
Carnival Corp	Employee PII + PHI	Unknown
Virgin Media	PII	900,000
Orsegups Particip	Tax Information	Unknown
Open Exchange Rates	PII and passwords	Unknown
European Union	PII CC info	Unknown
Blisk Borwser	California Gov email	2,900,000
Rogers Communicatuions	PII	Unknown
Tupperware	Stole customer payment info	Unknown
U. of Utah	Patient PII + PHI	Unknown
GE and Canon	Direct deposit info +PII	Unknown

A beacon of light in uncertain times.™

Breach Statistics – Verizon Breach Report

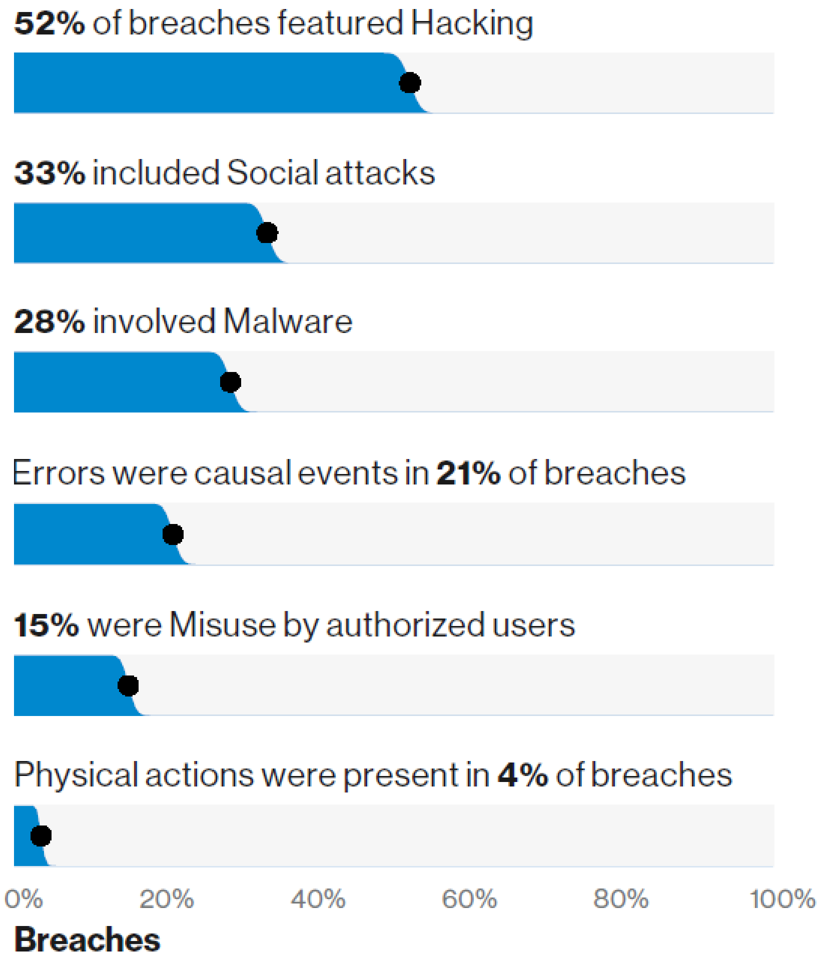


Figure 3. What tactics are utilized?

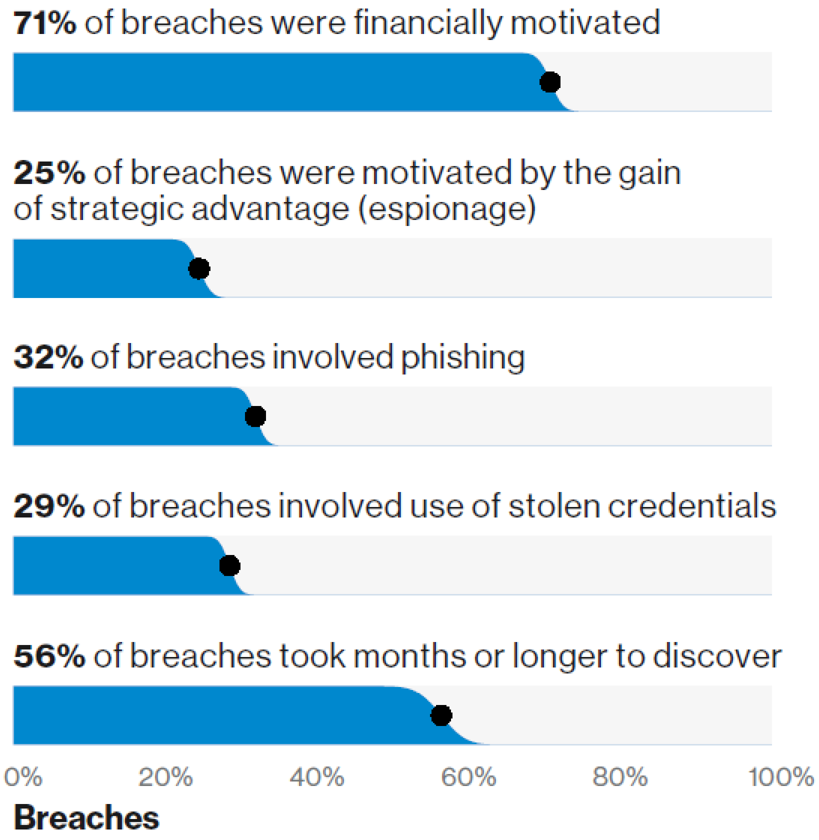


Figure 5. What are other commonalities?

A beacon of light in uncertain times.™

THREATS 2020 USSS-FBI

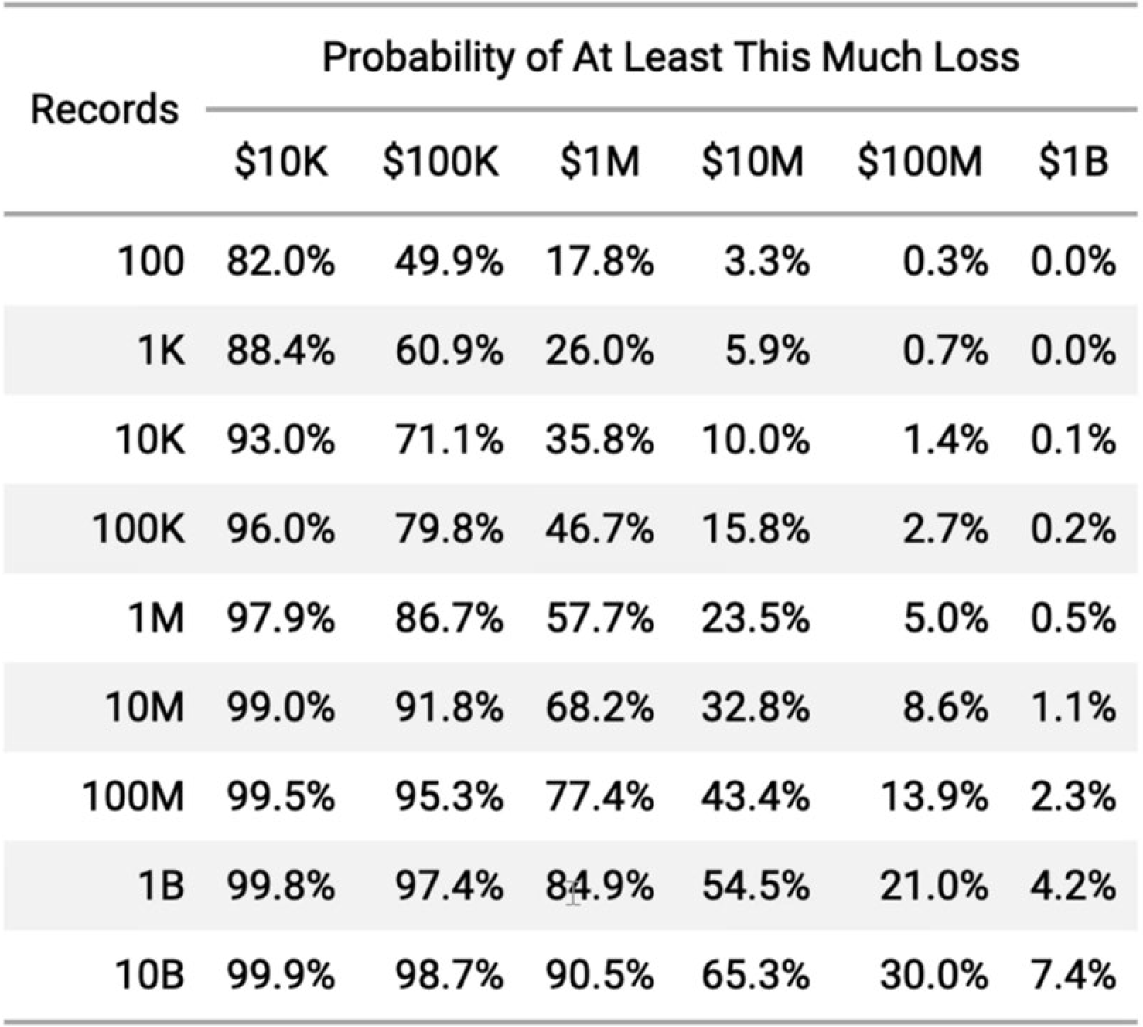
- Ransomware
- Phishing
- Business Email Compromise
- Stolen User Credentials
- Command and Control
- Crypto Jacking
- Stolen Data

Costs of a Data Breach Insurance Industry

This is based on actual claims data:

- Number of records are not the determinate factor.
- The type of record matters.
- The industry matters.
- The mitigation processes in place matter.

Source: Advison/Cyentia Institute March 2020



Records	Probability of At Least This Much Loss					
	$10K	$100K	$1M	$10M	$100M	$1B
100	82.0%	49.9%	17.8%	3.3%	0.3%	0.0%
1K	88.4%	60.9%	26.0%	5.9%	0.7%	0.0%
10K	93.0%	71.1%	35.8%	10.0%	1.4%	0.1%
100K	96.0%	79.8%	46.7%	15.8%	2.7%	0.2%
1M	97.9%	86.7%	57.7%	23.5%	5.0%	0.5%
10M	99.0%	91.8%	68.2%	32.8%	8.6%	1.1%
100M	99.5%	95.3%	77.4%	43.4%	13.9%	2.3%
1B	99.8%	97.4%	84.9%	54.5%	21.0%	4.2%
10B	99.9%	98.7%	90.5%	65.3%	30.0%	7.4%

A beacon of light in uncertain times.™

WHY DO WE COMMUNICATE

- Organized response—All pieces fit together.
- Inform your customers/suppliers/stakeholders.
- Update as matters merit.
- Meet statutory requirements.
- Address emotions and anticipate questions.

Guiding Principles of Communication

- Identify the facts as quickly as possible.
- Understand—"Why" we are communicating now—5 whys.
- Create pre-written messages.
- Leverage intelligence networks for critical metrics (if applicable).
- Update information as circumstances change.

Why we don’t communicate

- To assess blame, minimize, or deflect from magnitude
- To provide false hope that “we understand the magnitude”
- To appear more in control than you really are
- Know v. think v. hope
- Mitigation of liability—mitigation is a by-product of effective communication, not the purpose

But Don’t say …

- Statements that you don’t have proof are true
- That you know the depth of the breach (truism 1)
- That they will not be impacted (unless you know that to be true)
- What mitigation you are offering if you don’t know the scope of the breach
- You know how they feel
- Avoid “this will not define us” and canned crisis management lingo

Elements of a Cyber Incident Response Plan

- A plan is a *roadmap* of:
  - What should be done—steps and actions
  - When to do it—at point of the incident
  - Who should do it—roles and responsibilities

- A communications plan is integrated:
  - What do you say? Or **not** say!
  - Who do you say it to?
  - When do you say it?

First things First

- Communications should be part of the cyber incident response team, so they have the most recent unvarnished information.

- Start monitoring social media (remember fuzzy matches).

- Monitor the press.

- Look at your pre-written messages and start to craft messages.

Before the Breach

- Communication is part of your cyber incident response plan.
- Communication team—CEO, CIO/CISO, HR, IR, Legal, and Comms/PR
- Legal is not the leader for coordinating and crisis communications.
- Have a relationship with the media, law enforcement, and regulators (IGs are your representatives).
- Have draft communications and message maps.

A beacon of light in uncertain times.™

All Communications—Be prepared

- Nothing is private—expect leaks
- Pressures to disclose more than you know
- Positioning of your story by others
- Social media needs to be monitored

The three C's of Communications

- **Coordination**—Company will communicate internally to direct coordination activities regarding cybersecurity response and recovery.

- **Crisis**—Company will provide communications to address the potential crisis impacts on brand and reputation.

- **Compliance**—Company has communications responsibilities related to compliance notification to those parties who are impacted (or potentially impacted) by cybersecurity. These communications serve the dual purposes of notification and remedy actions to mitigate or prevent potential impacts.

Coordinating Communications

- Communications team needs to have “unvarnished” information from the cyber response team to assess communication/notification implications.

- Executive management will want written and oral communications detailing the cyber incident and plan of action, as needed.

- Evaluate appropriateness and traction of messages throughout the cyber incident by using “intelligence network” and metrics.

- Work with c-suite and operation leads to inquire, “what will your stakeholders want to know?”

TRUISM #1

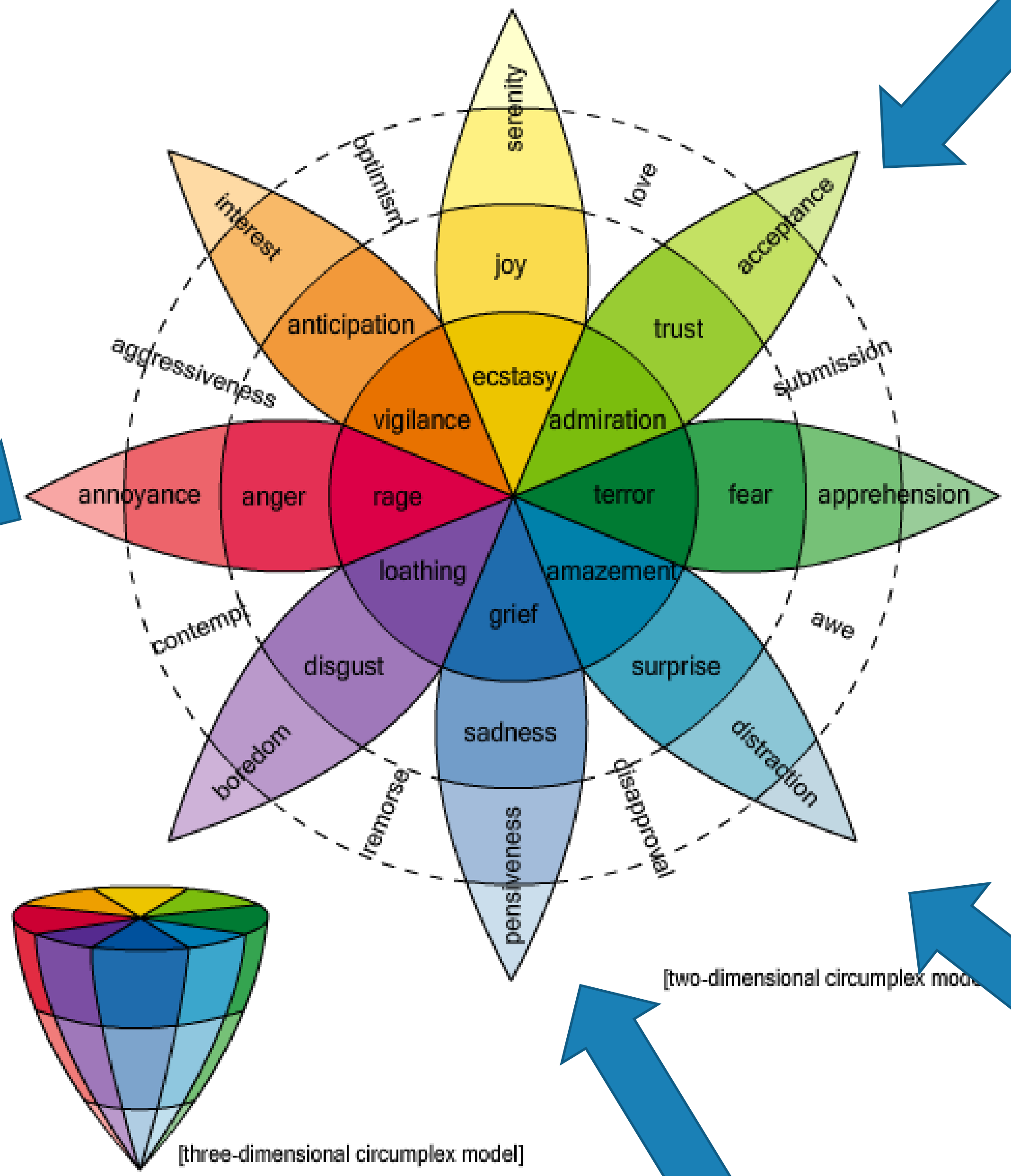
Half of What you know in the beginning of a crisis is wrong.

You just don't know which half!

EMOTIONS

BEAR HILL
ADVISORY GROUP

Plutchik's Wheel of Emotions



What emotions should we be addressing in coordinating communications?

Cybersecurity Communications Plan

Each element of your plan will include a communication element:

- **Coordinating communications** will apply to all elements.
- **Crisis communications** will apply to detection, containment, eradication, and recovery.
- **Compliance communication**: Detection and post-incident.

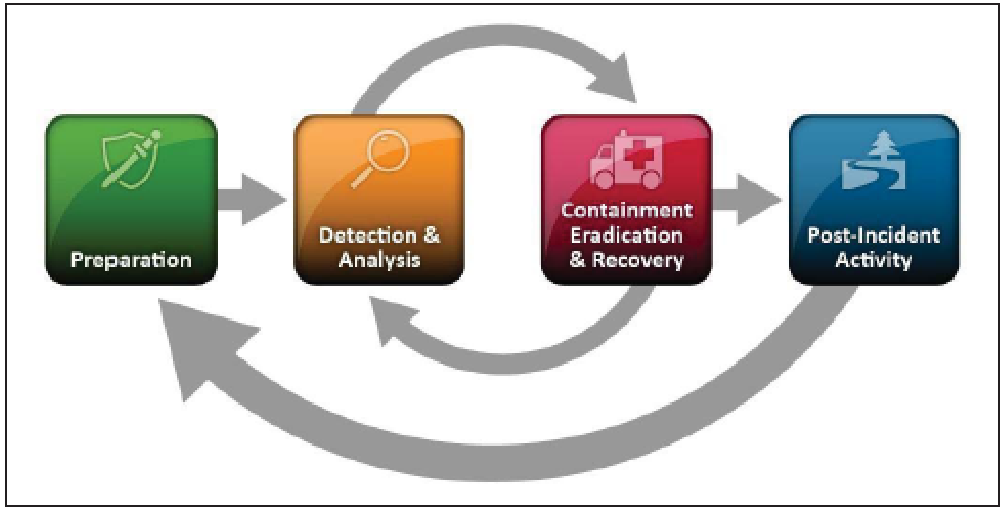


Figure 3-1. Incident Response Life Cycle

A beacon of light in uncertain times.™

COMM PLAN

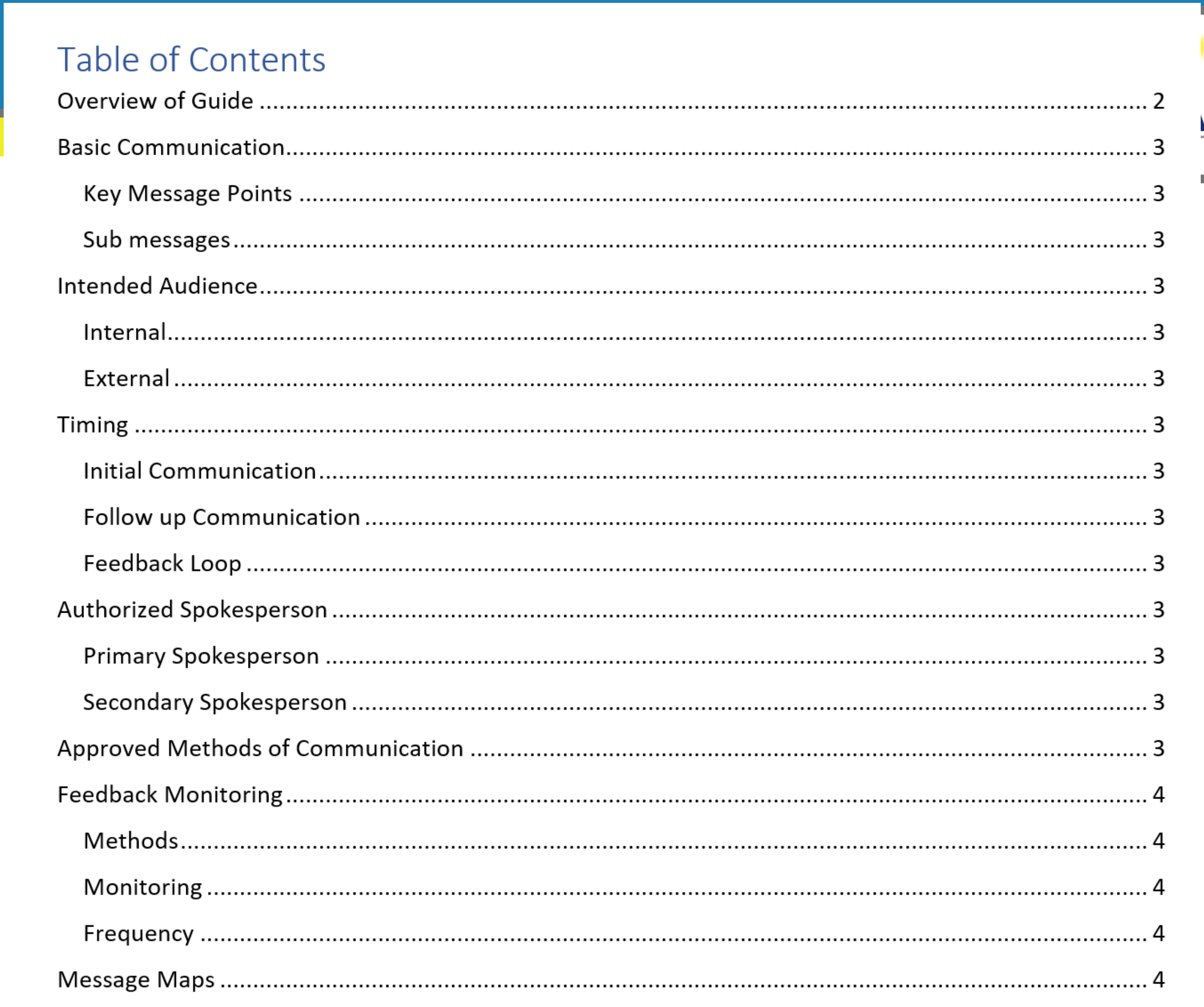


Table of Contents

A beacon of light in uncertain times.™

COMMUNICATION PLAN

- Overview—Objective, Scope, Assumptions, Life Plan Life Cycle, Comm Cycle
- Cyber Incident Crisis Communications Team—Roles, RACI Chart
- Team Activation
- Response Procedures—Planning, Alerting, Triage, Investigation, Containment, Eradiation
- Pre-Approved Message Maps
- Internal Communication Procedures—Blast Email, Phone/Text, Hotline, Intranet
- External Communication—Internet, Web Page
- Social Media—Rumor Control and Response

Know your audience- Coordinating

- Coordinating communications work best when they follow an escalation matrix.
- Seven parts to the communication:
  - What should I be doing?
  - Why am I doing it?
  - What will you be doing?
  - How long do I do it?
  - How will I know I'm done?
  - When will you talk with me next?
  - What do I do if I have questions?

COORDINATING COMMUNICATIONS- ESCALATION MATRIX

Cyber Incident Severity Escalation Matrix

Impacts	**Level 1 Guarded**	**Level 2 Elevated**	**Level 3 Severe**
Information Impact (Software, Network Database, and Access)	No information was exfiltrated, changed, deleted, or otherwise compromised	• Limited anomalies in monitoring and processing patterns • Multiple suspicious and possibly related tickets opened • Operational anomalies noted In systems or data	• Privacy breach sensitive PII of clients or employees breached • Proprietary breached unclassified proprietary information, potential critical Infrastructure information PCII was accessed, or exfiltrated • Integrity loss, sensitive proprietary information changed or deleted
Brand and Reputation (Traditional and Social Media)	Routine comments regarding company	Multiple postings regarding operational difficulties	• Brand attack on company Cyber action reported Employee/Client data posted on • Internet loss of PU or PHI reported, company problems reported, public awareness, or hack
Functional/ Operational Impact (Customer Experience, Internal/External)	No or minimal impact on organization ability to operate	• Organization has lost the ability to provide a critical service to a subset of internal or external customers • Business processes and/or function have degraded, or controls are not functioning as designed	Organization is no longer able to provide some critical services to any users
Data Recovery (Time, Effort, Ability)	Time to recovery is predictable and minimal	• Time to recover is predictable with additional resources • Time recovery is unpredictable; additional resources and outside help are needed • Data appears inaccurate or is not current	• All data lost • Data missing/manipulation • Inability to access Information • Recoverability not possible data exfiltrated and posted publicly • Launch investigation
Enterprise Support Actions	**Local Security Team LTRT Leads Response**	**Refer to CIRT/Notify CCCT LTRT Leads Response**	**ESCALATE to CIMT CIRL Leads Response**

COORDINATING- PREPARED

- Think about the different scenarios and anticipate messages.
- Focus on all departments’ communication needs.
- Technology, including “dark channel” need to be in place.
- Identifies all spokespeople and requires training.
- Requires testing of plan—tied to learning.

Detection- Coordination

BEAR HILL ADVISORY GROUP

- Typically first 24–48 hours—can be shorter/longer
- Which stakeholders have been impacted (you think)
- Communicate to leadership in coordination with IT security
- Verify classification of incident as operational/security
- Map game plan for communications strategy with legal and selected delivery mediums (website, email, social media)
- Remind the organization of your communication protocols

NOTE: Strategy of communications must be dynamic

Internal Communication

- Notification that cyber-incident response plan has been activated
- Refer to training company has undertaken and time to put into place
- Generally discuss incident—stick to what you know—don't guess—CIA
- Describe what systems might be impacted
- Give specific instructions for what you want them to do
- Remind staff of only authorized spokespeople

INTERNAL COMMUNICATION

- Assure group that customers and impacted third parties are top of mind and that notifications are being made or will be made, but that these need to come from authorized personnel.

- Ask for help in monitoring and provide method for feedback.

- Give schedule for next update and method (preferably live).

- Reiterate that you have prepared for this and now is time to pull together.

- Reinforce pride in brand and team.

Eradication/Recovery Coordination Communications

- This will be a high-stress and evolving stage—remember to keep cyber-incident response team and executive management informed on status of intelligence gathered.

- Where practical, make internal updates in person or via phone—restrict email dialogue.

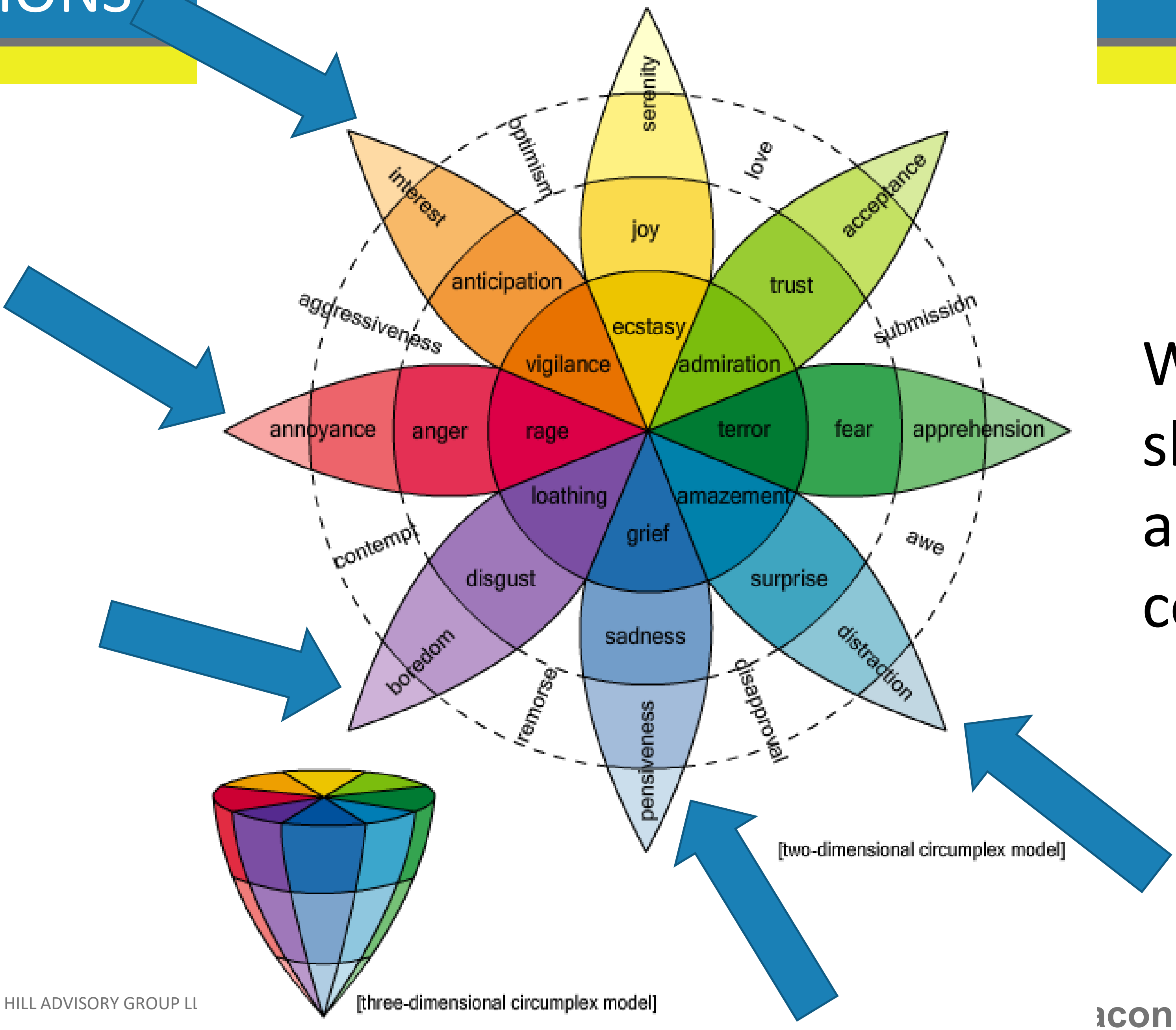
- Have a clear release protocol—make certain that everyone knows who has final release authority.

TRUISM #2

If you're explaining you're losing

EMOTIONS

Plutchik's Wheel of Emotions



[two-dimensional circumplex model]

[three-dimensional circumplex model]

What emotions should we be addressing in crisis communications?

CONSIDERATIONS WHEN BREACH CONFIRMED

- Do you want to provide a statement?
- Words have meaning—”incident” versus “breach”.
- Use words that people understand.
- Try to write at a fourth-grade level.

KNOW YOUR PRIORITIES

- Associates must be informed and armed with clear FAQs.
- Customers should be your touchstone—what would you want a supplier to do for you if you were in this situation?
- All communications must be controlled.
- Simultaneously with customer communications, notify AGs and regulators.
- Be prepared for the press.

Know your audience- Crisis Communication

BEAR HILL
ADVISORY GROUP

- Communications need to address their concerns.
- What happened?
- What are you going to FOR THEM?
- When will you talk with them next?
- How do they talk with you (call center, web page)?
- Have written script FAQs for all management and client contact.

A beacon of light in uncertain times.™

Crisis Communications

- What happened in nontechnical speak
- Who have you engaged to assist?
- Steps taken and being taken
- Promise for updates
- Don’t speculate or guess

DETECTION-CRISIS

- Detection stage is inherently confusing.
- Go into “lock down mode”.
    - No social media posting until clarity can be ascertained.
    - Keep record of all media calls and return calls at appropriate time.
    - Use crisis messaging.
    - Begin monitoring of media including social media.
- Legal should be part of all decisions.

Eradication/Recovery Crisis Comm

- Distribute official message to business operations and clients, as appropriate, for their use with incoming calls/emails, as appropriate at this time.
- Coordinate with the operational presidents to ensure that clients are kept informed throughout the event.
  - Provide impacted business operation with approved message to employees and clients regarding the event. Be certain this communication meets country-of-origin laws.
  - Ensure that outgoing voice messages provide accurate, up-to-date information for callers.

Crisis/ Regulatory Post Communications

- Prepare a “fact sheet” and update website contemporaneously with any release of information.
- Legal and finance may request that copy of public releases be filed as 8-K with SEC.
- Create a “dissemination control” so that you know what you released, to whom, and when.
- Many times, no outside information is released until after a thorough investigation.

Crisis Communications

BEAR HILL
ADVISORY GROUP

- Before you communicate, be certain to “close the loop” on your message.

- Have you addressed the emotional aspects of your audience?

- Be careful to coordinate with compliance so that you don’t inadvertently trigger a time line.

- Be careful if in a regulated industry—HIPPA/FINRA.

Crisis Communications-

BEAR HILL
ADVISORY GROUP

- Continue to communicate throughout the investigation.
- When final report is issued, share results, lessons learned, and steps taken.
- At each step, show the importance of your commitment to your customers.
- Similar message should be sent to associates.

CRISIS COMMUNICATIONS—REVIEW

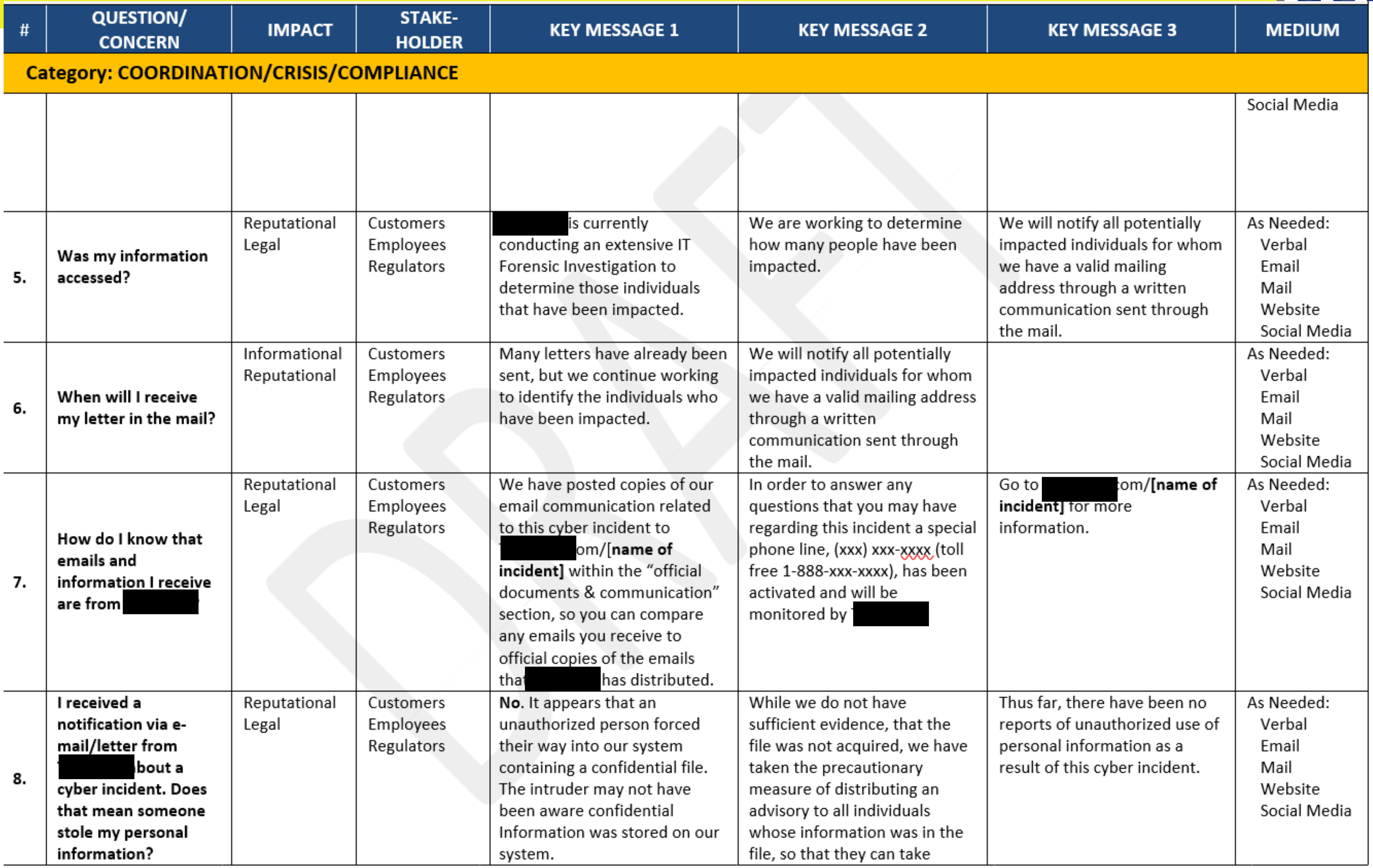
- Communicate liberally
- Blueprint to gather facts
- Have a designated spokesperson
- Names and numbers of all contacts (LE, Management, banks, media, etc.).
- Information hotline
- A single group email address
- Offsite communications center
- Counter rumors and speculation of facts

What do you say- Message Map

BEAR HILL ADVISORY GROUP

#	QUESTION/ CONCERN	IMPACT	STAKE-HOLDER	KEY MESSAGE 1	KEY MESSAGE 2	KEY MESSAGE 3	MEDIUM
Category: COORDINATION/CRISIS/COMPLIANCE							
1.	**What happened?**	Reputational	Customers Employees Regulators	In <inset month, year>, (Company) learned criminals forced their way into our system, gaining access to employee/customer PII/PHI information.	The information included names, mailing addresses, email addresses and/or phone numbers.	We have partnered with a leading third-party forensics firm who is thoroughly investigating the cyber incident.	As Needed: Verbal Email Mail Website Social Media
2.	**Has the issue been resolved?**	Reputational	Customers Employees Regulators	**Yes.** (Company) closed the access point that the criminals used when we discovered the cyber incident.	We have partnered with a leading third-party forensics firm who is thoroughly investigating the cyber incident.	We are contacting those who may have exposed information.	As Needed: Verbal Email Mail Website Social Media
3.	**What is a data breach?**	Informational	Customers Employees Regulators	A data breach or cyber incident is an event that occurs when secure information is inadvertently released to, or accessed by, unauthorized individuals.	Cyber incidents can include the loss or theft of information such as Personally Identifiable Information (PII), Personal Health Information (PHI), digital media, hard drives, and computers.	Other instances include situations where information is compromised due to security measures being breached or the unapproved posting or sharing of sensitive information via email or to public Internet sites.	As Needed: Verbal Email Mail Website Social Media

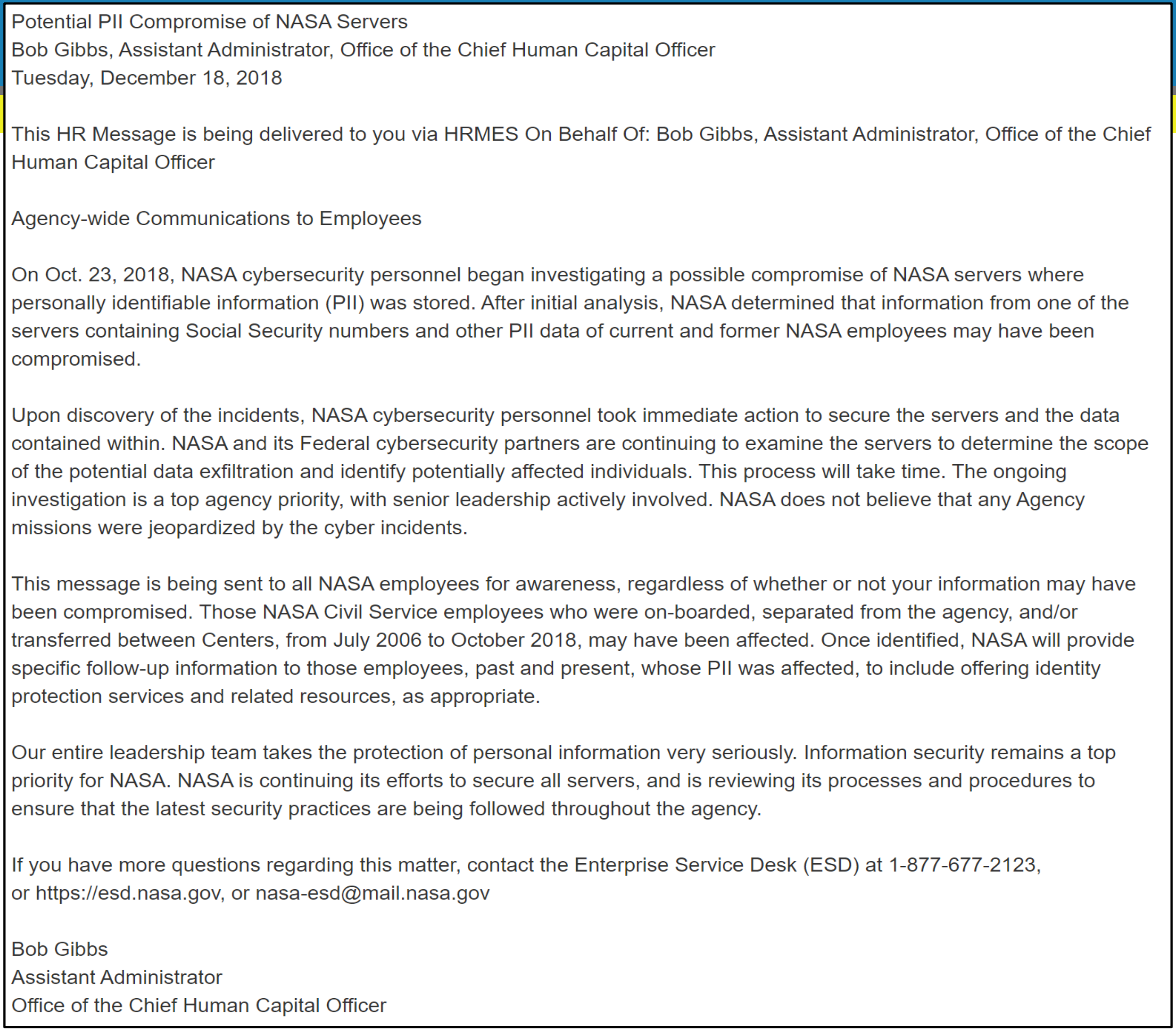
Message Maps



#	QUESTION/ CONCERN	IMPACT	STAKE-HOLDER	KEY MESSAGE 1	KEY MESSAGE 2	KEY MESSAGE 3	MEDIUM
Category: COORDINATION/CRISIS/COMPLIANCE							
							Social Media
5.	**Was my information accessed?**	Reputational Legal	Customers Employees Regulators	[redacted] is currently conducting an extensive IT Forensic Investigation to determine those individuals that have been impacted.	We are working to determine how many people have been impacted.	We will notify all potentially impacted individuals for whom we have a valid mailing address through a written communication sent through the mail.	As Needed: Verbal Email Mail Website Social Media
6.	**When will I receive my letter in the mail?**	Informational Reputational	Customers Employees Regulators	Many letters have already been sent, but we continue working to identify the individuals who have been impacted.	We will notify all potentially impacted individuals for whom we have a valid mailing address through a written communication sent through the mail.		As Needed: Verbal Email Mail Website Social Media
7.	**How do I know that emails and information I receive are from [redacted]**	Reputational Legal	Customers Employees Regulators	We have posted copies of our email communication related to this cyber incident to [redacted]om/**[name of incident]** within the "official documents & communication" section, so you can compare any emails you receive to official copies of the emails that [redacted] has distributed.	In order to answer any questions that you may have regarding this incident a special phone line, (xxx) xxx-xxxx (toll free 1-888-xxx-xxxx), has been activated and will be monitored by [redacted]	Go to [redacted]om/**[name of incident]** for more information.	As Needed: Verbal Email Mail Website Social Media
8.	**I received a notification via e-mail/letter from [redacted]bout a cyber incident. Does that mean someone stole my personal information?**	Reputational Legal	Customers Employees Regulators	**No.** It appears that an unauthorized person forced their way into our system containing a confidential file. The intruder may not have been aware confidential Information was stored on our system.	While we do not have sufficient evidence, that the file was not acquired, we have taken the precautionary measure of distributing an advisory to all individuals whose information was in the file, so that they can take	Thus far, there have been no reports of unauthorized use of personal information as a result of this cyber incident.	As Needed: Verbal Email Mail Website Social Media

A beacon of light in uncertain times.™

NASA



Potential PII Compromise of NASA Servers
Bob Gibbs, Assistant Administrator, Office of the Chief Human Capital Officer
Tuesday, December 18, 2018

This HR Message is being delivered to you via HRMES On Behalf Of: Bob Gibbs, Assistant Administrator, Office of the Chief Human Capital Officer

Agency-wide Communications to Employees

On Oct. 23, 2018, NASA cybersecurity personnel began investigating a possible compromise of NASA servers where personally identifiable information (PII) was stored. After initial analysis, NASA determined that information from one of the servers containing Social Security numbers and other PII data of current and former NASA employees may have been compromised.

Upon discovery of the incidents, NASA cybersecurity personnel took immediate action to secure the servers and the data contained within. NASA and its Federal cybersecurity partners are continuing to examine the servers to determine the scope of the potential data exfiltration and identify potentially affected individuals. This process will take time. The ongoing investigation is a top agency priority, with senior leadership actively involved. NASA does not believe that any Agency missions were jeopardized by the cyber incidents.

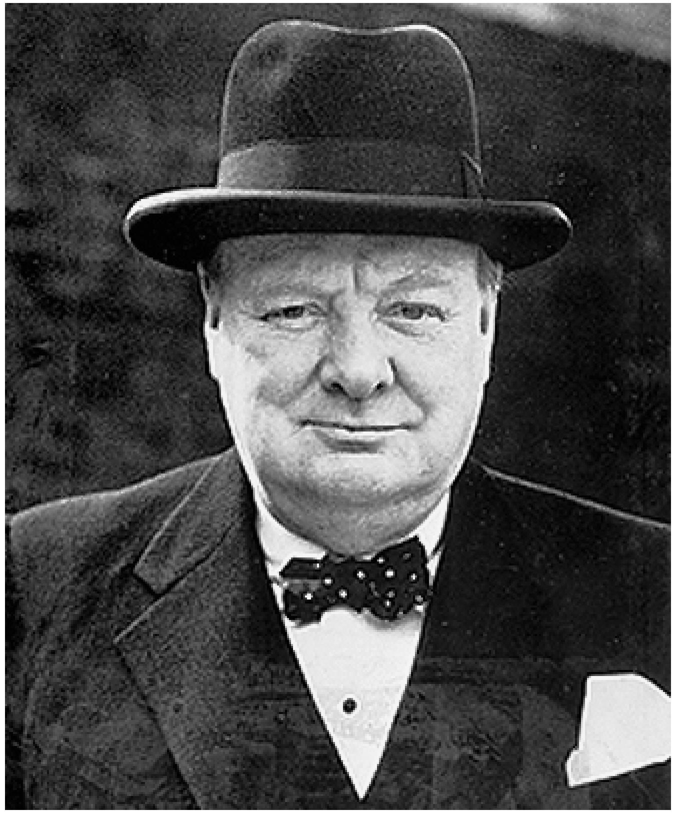
This message is being sent to all NASA employees for awareness, regardless of whether or not your information may have been compromised. Those NASA Civil Service employees who were on-boarded, separated from the agency, and/or transferred between Centers, from July 2006 to October 2018, may have been affected. Once identified, NASA will provide specific follow-up information to those employees, past and present, whose PII was affected, to include offering identity protection services and related resources, as appropriate.

Our entire leadership team takes the protection of personal information very seriously. Information security remains a top priority for NASA. NASA is continuing its efforts to secure all servers, and is reviewing its processes and procedures to ensure that the latest security practices are being followed throughout the agency.

If you have more questions regarding this matter, contact the Enterprise Service Desk (ESD) at 1-877-677-2123,
or https://esd.nasa.gov, or nasa-esd@mail.nasa.gov

Bob Gibbs
Assistant Administrator
Office of the Chief Human Capital Officer

Quote 2



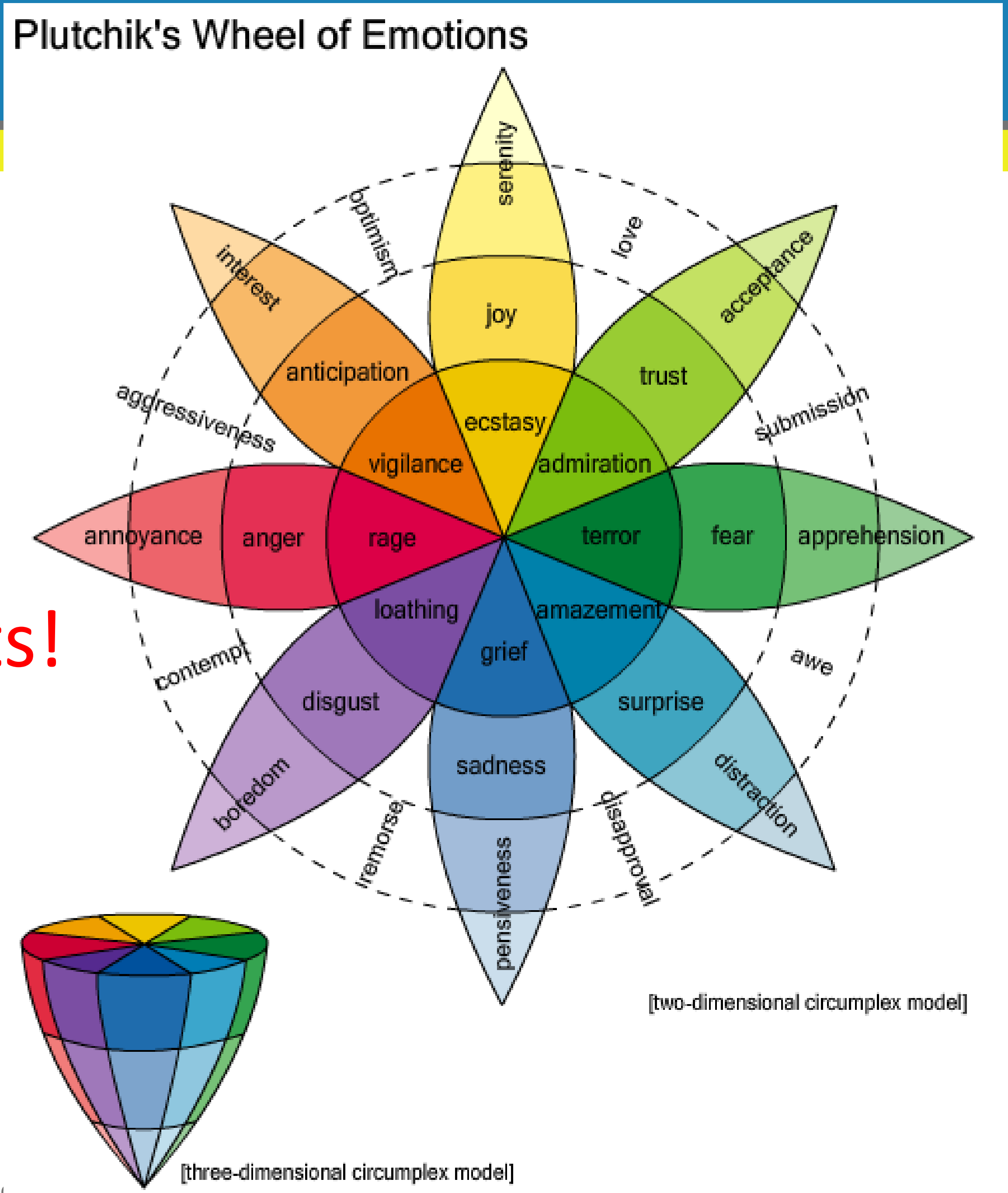
"All I want is compliance with my wishes, after reasonable discussion."

Winston Churchill

EMOTIONS

NONE!

Just the Facts!



Plutchik's Wheel of Emotions

[two-dimensional circumplex model]

[three-dimensional circumplex model]

What emotions should we be addressing in compliance communications?

DETECTION-COMPLIANCE

- Be careful at this stage regarding what you "know".
- Notifications may include third parties that may be the source of the incident.
- Law enforcement may be notified.
- Preliminary alerts to third parties and SMEs.

Recovery/Post Compliance Communications

- Be certain that method of notifications are in accordance with state and regulatory laws.

- Refrain from using email notification if a breach of PII or PHI is involved. Avoid re-victimization.

- Be prepared to handle returned mail—have a plan with legal on how you handle them.

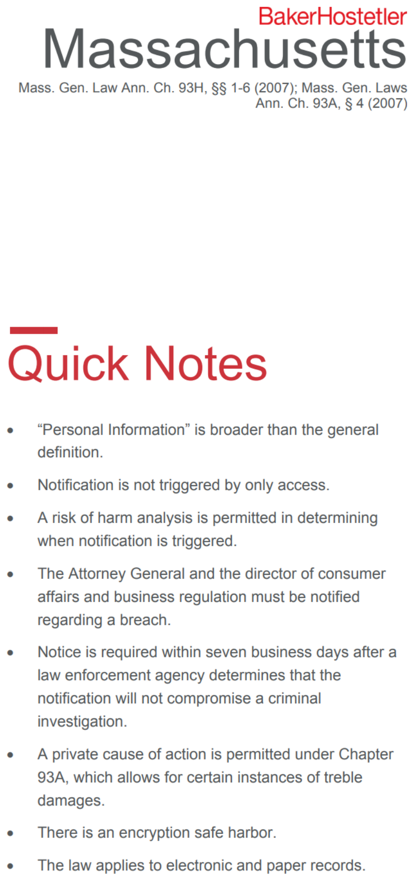
Know your audience- Compliance Communication

- Compliance now includes privacy laws as well as breach.
- CCPL, GDPR, others.
- Change frequently.
- Legal needs to drive which states/country notifications.
- Law firms should be consulted.

Notification

- As a general rule, notify when:
  - Unencrypted hardware is lost, stolen, or misplaced with sensitive data (PHI, PII).
  - Unauthorized access and exfiltrated data that could be sensitive.
  - Improper disposal of information and data of any form.
  - A third party has any of the above happen.
- As a general rule, you don’t need to notify when:
  - Information was retrieved before it was accessed.
  - Information is encrypted.
  - Information is limited to names and addresses.
  - Information is not accessed.

MASSACHUSETTS



BakerHostetler

Massachusetts

Mass. Gen. Law Ann. Ch. 93H, §§ 1-6 (2007); Mass. Gen. Laws Ann. Ch. 93A, § 4 (2007)

Quick Notes

- “Personal Information” is broader than the general definition.
- Notification is not triggered by only access.
- A risk of harm analysis is permitted in determining when notification is triggered.
- The Attorney General and the director of consumer affairs and business regulation must be notified regarding a breach.
- Notice is required within seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation.
- A private cause of action is permitted under Chapter 93A, which allows for certain instances of treble damages.
- There is an encryption safe harbor.
- The law applies to electronic and paper records.

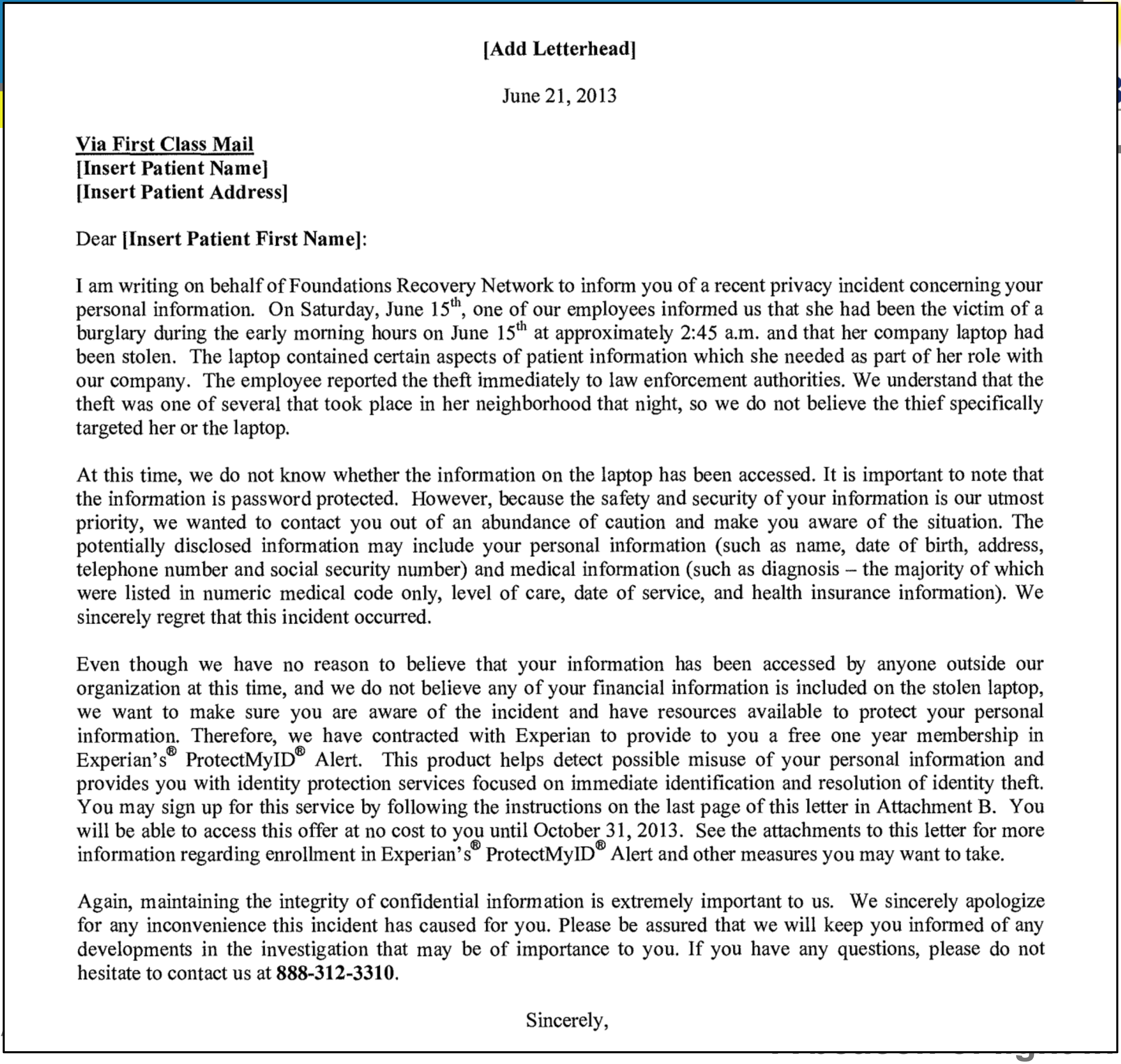
PII—SS#, DL, financial account with or w/out password.

Persons Covered—Person or agency that maintains, stores, owns, or licenses personal information about a resident of the commonwealth who knows of a breach of security, or has reason to know was acquired by an unauthorized person.

Encryption/Notification Trigger—Does not apply to encrypted information. Standard for triggering—know or have reason to know that info was obtained by an unauthorized user, or the info was acquired by an unauthorized user. The breach must create a substantial risk of identity theft or fraud against a person of the commonwealth.

Specific Content Requirements—Right to obtain a police report, request a security freeze, no charge for a security freeze, mitigation relief. Shall not include nature of breach, how many affected, or unauthorized access or use. Notice to AG will include details.

Timing—As soon as practical and without delay, but 7 days after law enforcement has been notified and determined there has been a breach.



[Add Letterhead]

June 21, 2013

<u>Via First Class Mail</u>
[Insert Patient Name]
[Insert Patient Address]

Dear **[Insert Patient First Name]**:

I am writing on behalf of Foundations Recovery Network to inform you of a recent privacy incident concerning your personal information. On Saturday, June 15th, one of our employees informed us that she had been the victim of a burglary during the early morning hours on June 15th at approximately 2:45 a.m. and that her company laptop had been stolen. The laptop contained certain aspects of patient information which she needed as part of her role with our company. The employee reported the theft immediately to law enforcement authorities. We understand that the theft was one of several that took place in her neighborhood that night, so we do not believe the thief specifically targeted her or the laptop.

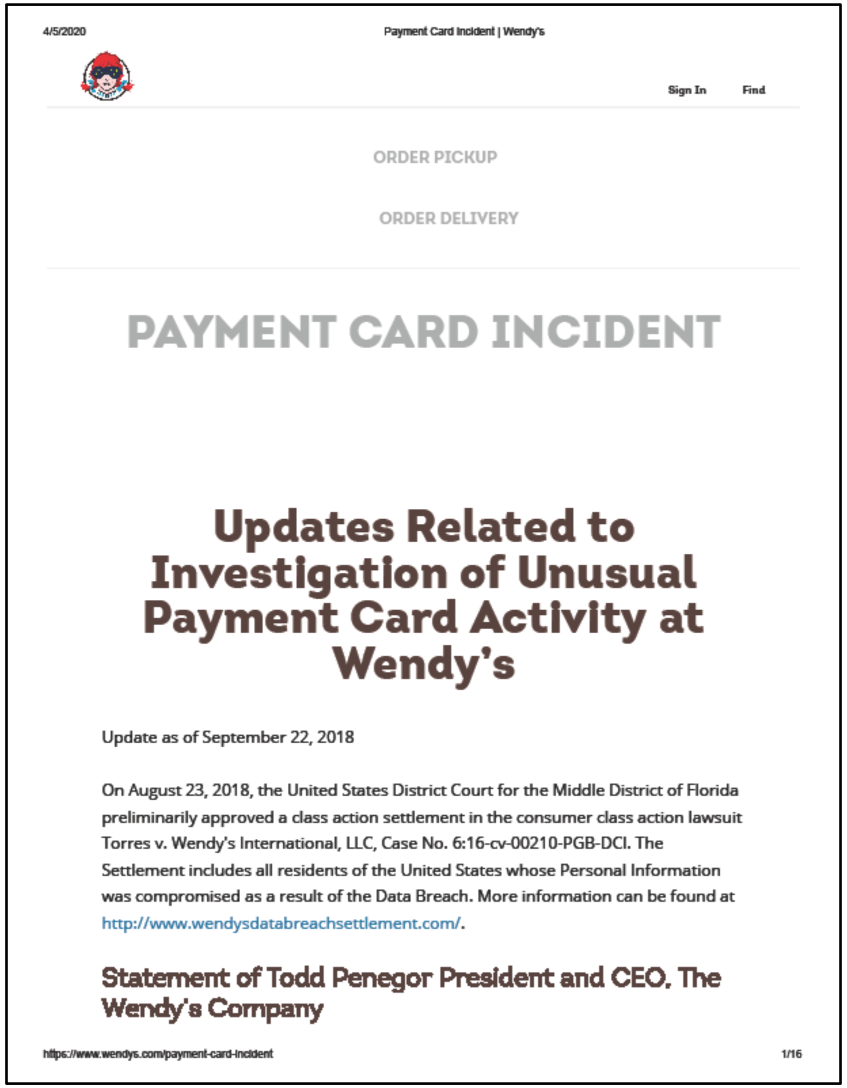
At this time, we do not know whether the information on the laptop has been accessed. It is important to note that the information is password protected. However, because the safety and security of your information is our utmost priority, we wanted to contact you out of an abundance of caution and make you aware of the situation. The potentially disclosed information may include your personal information (such as name, date of birth, address, telephone number and social security number) and medical information (such as diagnosis – the majority of which were listed in numeric medical code only, level of care, date of service, and health insurance information). We sincerely regret that this incident occurred.

Even though we have no reason to believe that your information has been accessed by anyone outside our organization at this time, and we do not believe any of your financial information is included on the stolen laptop, we want to make sure you are aware of the incident and have resources available to protect your personal information. Therefore, we have contracted with Experian to provide to you a free one year membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. You may sign up for this service by following the instructions on the last page of this letter in Attachment B. You will be able to access this offer at no cost to you until October 31, 2013. See the attachments to this letter for more information regarding enrollment in Experian's® ProtectMyID® Alert and other measures you may want to take.

Again, maintaining the integrity of confidential information is extremely important to us. We sincerely apologize for any inconvenience this incident has caused for you. Please be assured that we will keep you informed of any developments in the investigation that may be of importance to you. If you have any questions, please do not hesitate to contact us at **888-312-3310**.

Sincerely,

WENDY'S



4/5/2020 Payment Card Incident | Wendy's

Sign In Find

ORDER PICKUP

ORDER DELIVERY

PAYMENT CARD INCIDENT

Updates Related to Investigation of Unusual Payment Card Activity at Wendy's

Update as of September 22, 2018

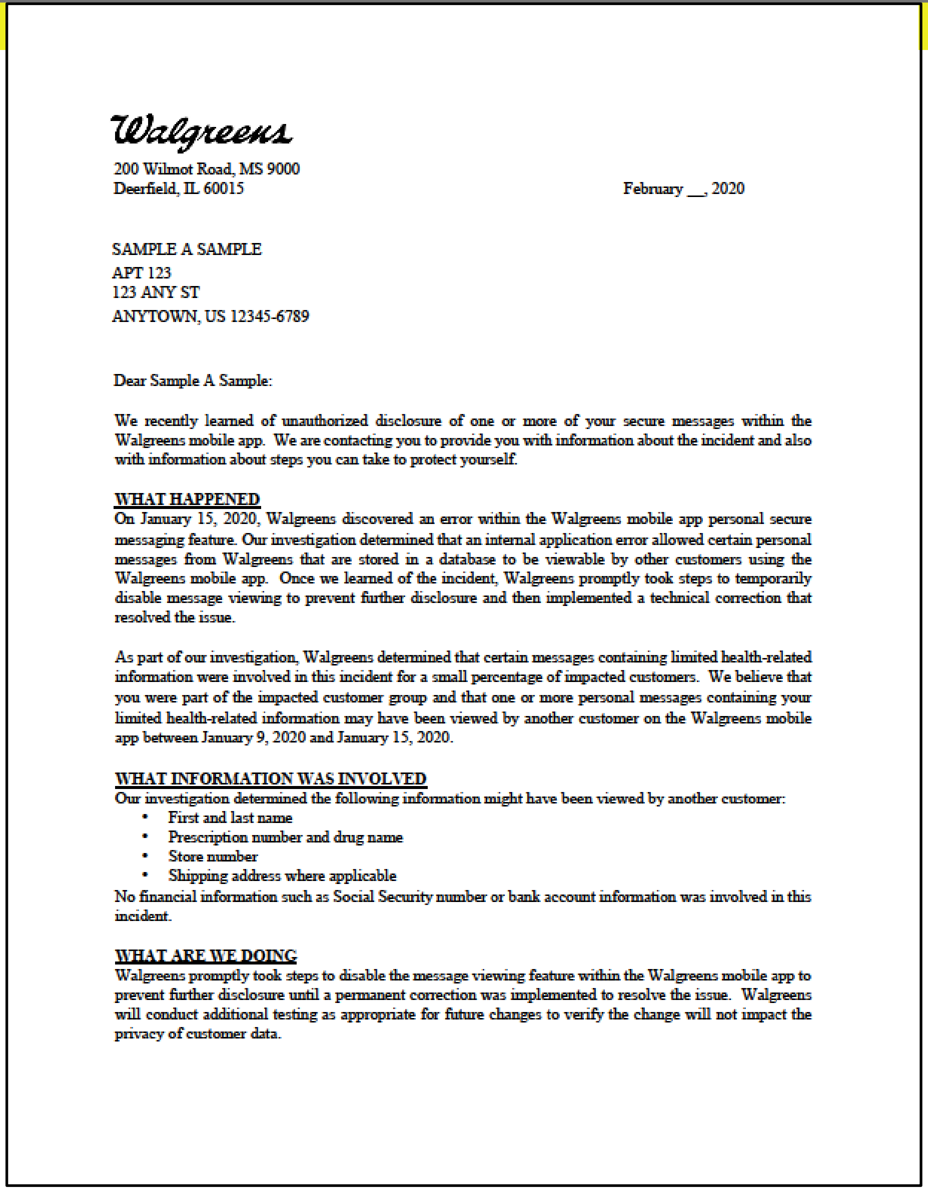
On August 23, 2018, the United States District Court for the Middle District of Florida preliminarily approved a class action settlement in the consumer class action lawsuit Torres v. Wendy's International, LLC, Case No. 6:16-cv-00210-PGB-DCI. The Settlement includes all residents of the United States whose Personal Information was compromised as a result of the Data Breach. More information can be found at http://www.wendysdatabreachsettlement.com/.

Statement of Todd Penegor President and CEO, The Wendy's Company

https://www.wendys.com/payment-card-incident 1/16

WALGREENS

BEAR HILL
ADVISORY GROUP



Walgreens

200 Wilmot Road, MS 9000
Deerfield, IL 60015

February __, 2020

SAMPLE A SAMPLE
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

We recently learned of unauthorized disclosure of one or more of your secure messages within the Walgreens mobile app. We are contacting you to provide you with information about the incident and also with information about steps you can take to protect yourself.

WHAT HAPPENED

On January 15, 2020, Walgreens discovered an error within the Walgreens mobile app personal secure messaging feature. Our investigation determined that an internal application error allowed certain personal messages from Walgreens that are stored in a database to be viewable by other customers using the Walgreens mobile app. Once we learned of the incident, Walgreens promptly took steps to temporarily disable message viewing to prevent further disclosure and then implemented a technical correction that resolved the issue.

As part of our investigation, Walgreens determined that certain messages containing limited health-related information were involved in this incident for a small percentage of impacted customers. We believe that you were part of the impacted customer group and that one or more personal messages containing your limited health-related information may have been viewed by another customer on the Walgreens mobile app between January 9, 2020 and January 15, 2020.

WHAT INFORMATION WAS INVOLVED

Our investigation determined the following information might have been viewed by another customer:

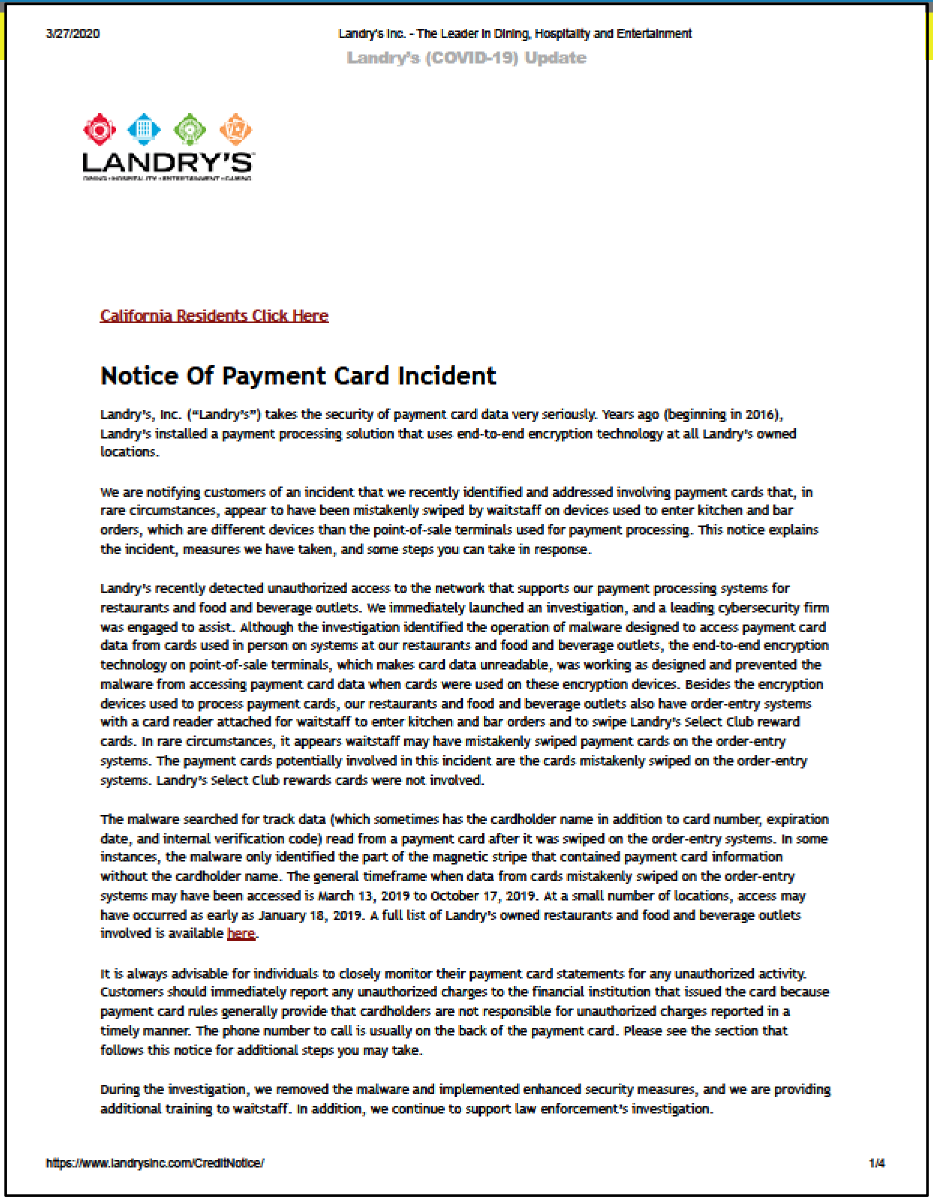
- First and last name
- Prescription number and drug name
- Store number
- Shipping address where applicable

No financial information such as Social Security number or bank account information was involved in this incident.

WHAT ARE WE DOING

Walgreens promptly took steps to disable the message viewing feature within the Walgreens mobile app to prevent further disclosure until a permanent correction was implemented to resolve the issue. Walgreens will conduct additional testing as appropriate for future changes to verify the change will not impact the privacy of customer data.

LANDRY'S



3/27/2020 Landry's Inc. - The Leader In Dining, Hospitality and Entertainment

Landry's (COVID-19) Update

LANDRY'S

California Residents Click Here

Notice Of Payment Card Incident

Landry's, Inc. ("Landry's") takes the security of payment card data very seriously. Years ago (beginning in 2016), Landry's installed a payment processing solution that uses end-to-end encryption technology at all Landry's owned locations.

We are notifying customers of an incident that we recently identified and addressed involving payment cards that, in rare circumstances, appear to have been mistakenly swiped by waitstaff on devices used to enter kitchen and bar orders, which are different devices than the point-of-sale terminals used for payment processing. This notice explains the incident, measures we have taken, and some steps you can take in response.

Landry's recently detected unauthorized access to the network that supports our payment processing systems for restaurants and food and beverage outlets. We immediately launched an investigation, and a leading cybersecurity firm was engaged to assist. Although the investigation identified the operation of malware designed to access payment card data from cards used in person on systems at our restaurants and food and beverage outlets, the end-to-end encryption technology on point-of-sale terminals, which makes card data unreadable, was working as designed and prevented the malware from accessing payment card data when cards were used on these encryption devices. Besides the encryption devices used to process payment cards, our restaurants and food and beverage outlets also have order-entry systems with a card reader attached for waitstaff to enter kitchen and bar orders and to swipe Landry's Select Club reward cards. In rare circumstances, it appears waitstaff may have mistakenly swiped payment cards on the order-entry systems. The payment cards potentially involved in this incident are the cards mistakenly swiped on the order-entry systems. Landry's Select Club rewards cards were not involved.

The malware searched for track data (which sometimes has the cardholder name in addition to card number, expiration date, and internal verification code) read from a payment card after it was swiped on the order-entry systems. In some instances, the malware only identified the part of the magnetic stripe that contained payment card information without the cardholder name. The general timeframe when data from cards mistakenly swiped on the order-entry systems may have been accessed is March 13, 2019 to October 17, 2019. At a small number of locations, access may have occurred as early as January 18, 2019. A full list of Landry's owned restaurants and food and beverage outlets involved is available here.

It is always advisable for individuals to closely monitor their payment card statements for any unauthorized activity. Customers should immediately report any unauthorized charges to the financial institution that issued the card because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card. Please see the section that follows this notice for additional steps you may take.

During the investigation, we removed the malware and implemented enhanced security measures, and we are providing additional training to waitstaff. In addition, we continue to support law enforcement's investigation.

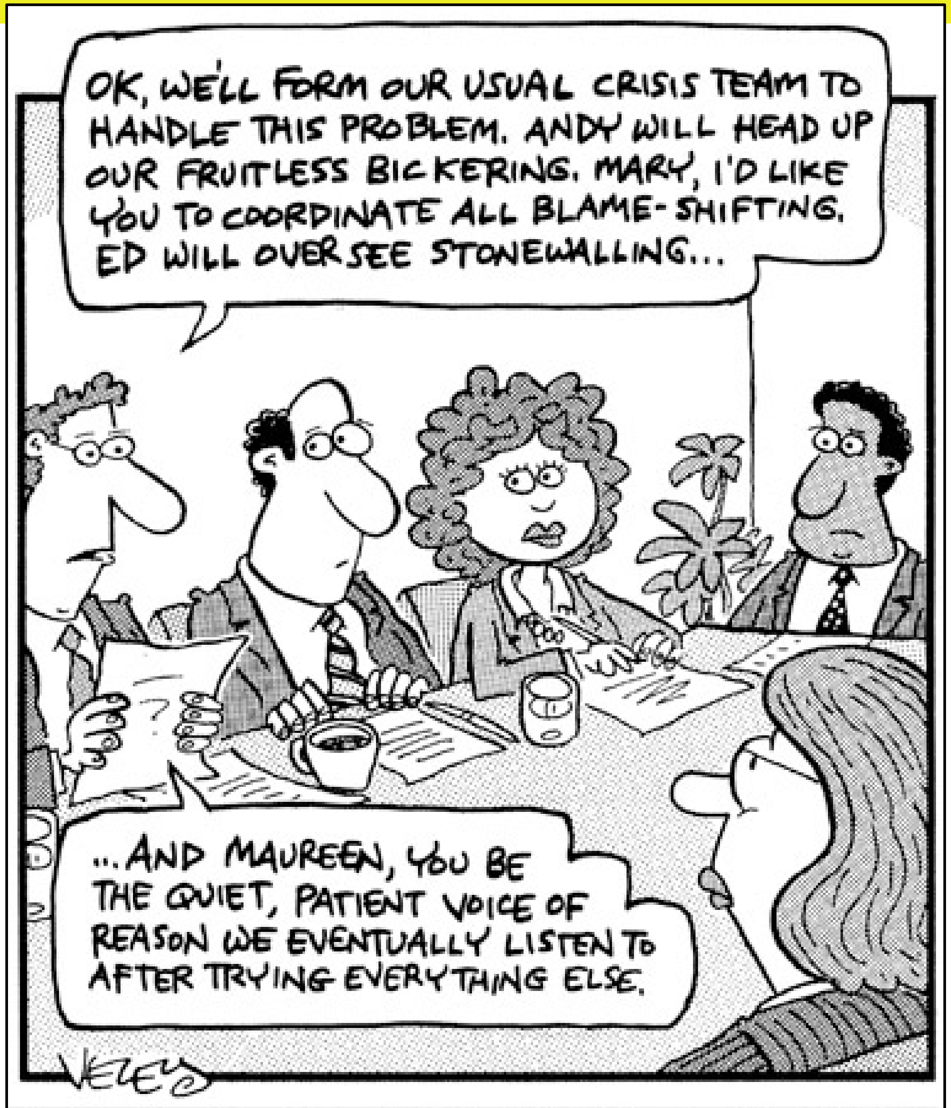
https://www.landrysinc.com/CreditNotice/ 1/4

A beacon of light in uncertain times.™

Best Practices

- Always have legal and CEO approve messages.
- Prepare talking points for key individuals, referring to spokesperson, release.
- Know your “core anchor message”.
- Coordinate the releases.
- Always inform state AGs impacted when you release information. They will be called!

In Summary


OK, WE'LL FORM OUR USUAL CRISIS TEAM TO HANDLE THIS PROBLEM. ANDY WILL HEAD UP OUR FRUITLESS BICKERING. MARY, I'D LIKE YOU TO COORDINATE ALL BLAME-SHIFTING. ED WILL OVERSEE STONEWALLING...
...AND MAUREEN, YOU BE THE QUIET, PATIENT VOICE OF REASON WE EVENTUALLY LISTEN TO AFTER TRYING EVERYTHING ELSE.

Reprinted from Funny Times / PO Box 18530 / Cleveland Hts. OH 44118
phone: 216.371.8600 / email: ft@funnytimes.com

Questions and Contact Information

Jack P. Healey CFE, CPA/CFF

CEO
Bear Hill Advisory Group
770.362.2008
JHEALEY@BHAGRP.COM

@CyberBizRescue
@BHAGRP

www.bhagrp.com

A beacon of light in uncertain times.™

Multi-dimensional Cyber Communications-
More than Just Notification and Compliance

Supplemental Information
June 2020

BEAR HILL
ADVISORY GROUP

VIRTUAL CONFERENCE

ACFE GLOBAL

FRAUD CONFERENCE

JUNE 22–24, 2020 | ONLINE VIRTUAL CONFERENCE

ACFE

Association of Certified Fraud Examiners

Multi-Dimensional Cyber Communications: It’s More Than Notification and Compliance

Jack Healey, CFE, CPA, CFF, CRISC

Chief Executive Officer

Bear Hill Advisory Group

LIGHT the WAY