# Agenda Summary Report (ASR)

## Franklin County Board of Commissioners

| | |
|---|---|
| **DATE SUBMITTED:** 01/28/2020 | **PREPARED BY:** Shirley Jones |
| **Meeting Date Requested:** 02/04/2020 | **PRESENTED BY:** Keith Johnson |
| **ITEM:** (Select One) X Consent Agenda | ☐ Brought Before the Board<br>Time needed: |
| **SUBJECT: Approval of Franklin County Data Breach Response Plan** | |
| **FISCAL IMPACT:** $0, approval of response plan. | |

**BACKGROUND:**

PRELIMINARY CONSIDERATIONS

- Responding to a data breach that exposes individuals' personally identifiable information (PII) typically involves the following stages:
  - verification;
  - containment and mitigation;
  - investigation and analysis;
  - notification; and
  - post-notification, including a review of the breach to improve processes.
- Data breach response is typically not purely linear, as these stages and the activities associated with these stages frequently overlap.
- Keep a record of any actions you take in responding to the incident. Use the Data Breach Forms. Some laws, including the Health Insurance Portability and Accountability Act (HIPAA), may require keeping an incident log.
- Preserve any evidence that may be relevant to any potential regulatory investigation or litigation.

**RECOMMENDATION:**

Approval of Data Breach Response Plan for implementation in Franklin County should the need arise.

**COORDINATION:**

Keith Johnson, Administrator
Jen Johnson, Deputy Prosecuting Attorney
Kevin Scott, IS Director

**ATTACHMENTS: (Documents you are submitting to the Board)**

ASR/Resolution/Data Breach Response Plan

**HANDLING / ROUTING: (Once document is fully executed it will be imported into Document Manager. Please list name(s) of parties that will need a pdf)**

Administrator's Office, Prosecuting Attorney's Office, IS

*I certify the above information is accurate and complete.*

Keith Johnson, Administrator

# FRANKLIN COUNTY RESOLUTION _____

BEFORE THE BOARD OF COMMISSIONERS
FRANKLIN COUNTY, WASHINGTON

***APPROVAL OF THE DATA BREACH RESPONSE PLAN***

**WHEREAS,** a proactive Data Breach Response Plan is beneficial to Franklin County regarding any potential exposure of sensitive information;

**WHEREAS,** pursuant to RCW 36.01.010 and RCW 36.32.120, the legislative authority of Franklin County is authorized to act on behalf of the County and ensure the care of County property and management of County funds and business; and

**NOW, THEREFORE, BE IT RESOLVED,** that the Franklin County Commissioners constitute the legislative authority of Franklin County and desire to approve the Data Breach Response Plan as being in the best interest of Franklin County.

**APPROVED** this 4th day of February 2020.

BOARD OF COUNTY COMMISSIONERS
**FRANKLIN COUNTY**, WASHINGTON

_____
Chair

_____
Chair Pro Tem

_____
Member

***ATTEST:***

_____
Clerk to the Board

# DATA BREACH RESPONSE PLAN

## PRELIMINARY CONSIDERATIONS

- Responding to a data breach that exposes individuals' personally identifiable information (PII) typically involves the following stages:
  - verification;
  - containment and mitigation;
  - investigation and analysis;
  - notification; and
  - post-notification, including a review of the breach to improve processes.
- Data breach response is typically not purely linear, as these stages and the activities associated with these stages frequently overlap.
- Keep a record of any actions you take in responding to the incident. Use the Data Breach Forms. Some laws, including the Health Insurance Portability and Accountability Act (HIPAA), may require keeping an incident log.
- Preserve any evidence that may be relevant to any potential regulatory investigation or litigation.

## VERIFY THE DATA BREACH

- Identify the affected systems or hardware (such as a lost laptop or USB drive).
- Determine the nature of the data maintained in those systems or on the hardware.
- Determine the type of incident, such as whether the disclosure was:
  - internal or external;
  - caused by a company insider or outside actor; and
  - the result of a malicious attack or an accident.
- Determine whether the incident exposed or is reasonably likely to have exposed data.
- Determine whether PII was affected and the data elements possibly at risk, such as name, date of birth, or Social Security number.
- IT department personnel should fill out the Data Breach Forms so that information is available in one place for government agencies and insurance companies.
- CONTACT THE INFORMATION SERVICES DEPARTMENT AND THE RISK MANAGER IMMEDIATELY

## CONTAIN AND MITIGATE THE DATA BREACH- INFORMATION SERVICES DEPARTMENT

As soon as a IS department verifies a breach has occurred, it should take all necessary steps to contain the incident and limit further data loss or intrusion, such as:

- Identify the system, application, and information compromised.
- Identify and take immediate action to stop the source or entity responsible, for example by:
  - taking affected machines offline;
  - segregating affected systems;
  - deleting hacker tools; and
  - immediately securing the area if the breach involves a physical security breach.
- Determine whether other systems are under threat of immediate or future danger.
- Determine whether to implement additional technical measures to contain the data breach, such as changing locks, passwords, administrative rights, access codes, or passwords.

## CONVENE THE DATA BREACH RESPONSE TEAM

- Convene the data breach response team when there is a reasonable belief that a breach may have occurred. The response team is responsible for:
  - managing and coordinating the county's overall response efforts; and
  - investigating and responding to the data breach in accordance with the county's incident response plan.
- The data breach response team generally should:
  - determine the scope of an internal investigation (see Investigate and Analyze the Data Breach);
  - collect data related to the breach (see Collect Data);
  - consider immediate notification of outside counsel,
  - consider whether and when to notify law enforcement or regulatory authorities (see Consider Communications with Regulators and Law Enforcement);
  - consider whether it should engage specialized third-party consultants to assist in capturing relevant information and performing a forensic analysis;
  - appoint someone responsible for keeping a response log that records the actions taken during the investigation;
  - institute and manage internal and external communications protocols (see Develop a Communications Plan) and
  - conduct follow up reviews on the effectiveness of the company's response to an actual attack (see Post-Notification and Breach Response Review)

## INVESTIGATE AND ANALYZE THE DATA BREACH

When investigating a data breach, the response team should:

- Institute communications protocols, such as communicating by telephone where possible, to prevent information leaks.
- Take steps to conduct the incident investigation under attorney- client privilege.
- Preserve all data and evidence, including forensic evidence, for later examination or if needed in the event of any later legal or regulatory action.

## COLLECT DATA

- Keep in mind that collecting data is a continuous process.
- To effectively collect relevant data, the county will likely have work with its IT department or may engage a forensics vendor.
- Collect information about the breach itself, including:
  - how the breach was discovered;
  - the nature of the breach (for example, whether systems were compromised or hardware lost);
  - the date and time of the breach;
  - the duration and location of the breach;
  - the method of system intrusion;
  - the compromised systems or files; and
  - the compromised systems or files; and
  - whether PII was actually accessed.
- Collect details about the compromised data, including:
  - a list of affected individuals;
  - the affected data elements;
  - the number of records affected; and
  - whether any of the data was encrypted.

**ANALYZE THE LEGAL IMPLICATIONS- Prosecuting Attorney's Office**

- Once the basic facts are known, analyze the legal issues stemming from the breach. The legal analysis should be conducted at the direction of internal or external counsel.
- To assess whether the breach may trigger individual and regulatory notification obligations, in addition to the data elements affected, determine:
  - the likely use of or access to the compromised data;
  - for purposes of some laws, the likelihood of harm to individuals; and
  - the number of persons likely affected.
- Identify the jurisdictions where any affected persons may reside to assess which state (or foreign) breach notification laws may be triggered.
- Identify whether the type of data compromised, for instance medical information, triggers additional statutory obligations under state law.
- Identify whether the county is subject to sector-specific federal notification obligations, for instance if it is a HIPAA-covered entity.
- Review relevant contracts and policies.
- Based on the analysis of these factors, determine whether the breach triggers any notification obligations as to:
  - affected individuals;
  - CRIME VICTIMS: we MUST notify The Office of Crime Victims Advocacy within 24 hours in the event of a breach or detection of an imminent breach. Contact the OCVA & STOP Grant Managers.
  - Determine whether any other grants that the county is involved with require notification, and make required notification.
  - third-party business partners or vendors;
  - state attorney generals or other regulatory agencies, such as the Office of Civil Rights in the event of a HIPAA-covered breach
  - law enforcement or
  - consumer reporting agencies.
- Review insurance coverage to determine any relevant coverage and notify carriers.
- Determine the county's indemnification obligations or rights, including whether:
  - any third parties have any obligations to the county; and
  - the county has any indemnification obligations to third parties.
- Assess the risk of litigation or regulatory action against the county.
- Determine whether the county should take any employment action against any responsible employees as a result of the breach.

**DEVELOP A COMMUNICATIONS PLAN**

Before any communications, develop a communications plan approved by the county administrator and prosecuting attorney and/or outside counsel that:

- Ensures timely and coordinated execution of external communications and notifications.
- Avoids disseminating incomplete information or information that has not been thoroughly vetted.
- Addresses how the county responds to inquiries about the breach (see Prepare an Inquiry Response Plan).

- Tailors communications to each of the key audiences, including:
  - the county's employees (see Consider Internal Communications);
  - affected individuals (see Plan for Communications with Affected Individuals and Notification)
  - the media (see Plan for Media Communications)
  - vendors or other third parties (see Address Communications with Third Parties); and
  - law enforcement and regulators (see Consider Communications with Regulators and Law Enforcement).

**PREPARE AN INQUIRY RESPONSE PLAN**

- Develop an inquiry response plan that takes into account the size of the breach and the number of individuals affected.
- Ensure that the plan addresses:
  - whether to handle inquiries internally or by engaging a call center vendor;
  - whether to post a statement on the county's website, which in some cases may be required by law; and
  - the methods of communication with each of the key audience groups

**CONSIDER INTERNAL COMMUNICATIONS**

In communicating with employees:

- Limit communications regarding the details of the incident on a need-to-know basis.
- Notify employees as soon as the data breach is contained and basic facts are known.
- Consider whether employees are also affected persons that must receive individual notification.
- Issue a policy statement to employees regarding external communication with media or third parties.

**PLAN FOR MEDIA COMMUNICATIONS**

- Attempt to avoid news of the data breach reaching the media before notifying affected individuals (see Notification)
- Prepare a media holding statement to ensure that the county is prepared to make an announcement quickly if required.
- Draft a media and web statement or press release based on incident-specific facts.
- Designate a contact person on the data breach response team to handle media and law enforcement inquiries.

**CONSIDER COMMUNICATIONS WITH REGULATORS AND LAW ENFORCEMENT**

- Consider whether and when to contact law enforcement (see Practice Note, Breach Notification: Contacting Law Enforcement)
- Keep in mind that law enforcement authorities may require a delay in the notification to affected persons or a release of public information if those activities may hamper law enforcement investigations.
- Consider whether the county must, or if it is otherwise advisable to, communicate with any regulatory authority regarding the incident.
- Both counsel and the county administration should be included in developing communications with regulators.

**ADDRESS COMMUNICATIONS WITH THIRD PARTIES**

If the data breach affected PII the county maintains for third- parties:

- Involve County administration and counsel in developing the approach to communications.
- Reach out to data owners as soon as possible.
- Pre-determine whether:
  - individual notification may be necessary; and

- the county must by contract or is otherwise willing to notify on the data owner's behalf.
- Foster a cooperative relationship with the data owners to secure sensitive data and mitigate the damage that may arise from the data breach.
- Designate an individual on the data breach response team to handle communications with data owners and other affected third parties.

## PLAN FOR COMMUNICATIONS WITH AFFECTED PERSONS

- Prepare for inquiries from affected individuals after the breach becomes public, usually at the time that notification is sent (see Prepare an Inquiry Response Plan).
- An effective communications plan should include, as appropriate based on the scope of the breach:
  - setting up a dedicated phone number to field calls and questions from affected individuals;
  - preparing a call center script, training call center representatives, and establishing an escalation process for inquiries that the front-line call center cannot handle ;
  - preparing frequently asked questions (FAQs) for responding to affected individuals' inquiries;
  - posting information on the county's website; and
  - designating an individual from the data breach response team to field inquiries that do not come through the designated number.

## NOTIFICATION

If notification is necessary:

- Develop a notification plan (see Prepare a Notification Plan)
- Ensure that notification is executed in a timely and legally sufficient manner (see Execute the Notification Plan)

## PREPARE A NOTIFICATION PLAN

- Identify notification obligations based on analysis of legal requirements (see Analyze the Legal Implications).
- Determine the parties or entities that should be notified before notification to affected individuals, such as:
  - law enforcement;
  - regulatory agencies or
  - credit reporting agencies
- Consider whether the county can handle notification logistics internally or whether it must engage third-party notification vendors for:
  - printing and mailing letters; or
  - operating a call center to respond to inquiries (see Prepare an Inquiry Response Plan)
- Determine whether to offer remediation services to affected individuals, such as:
  - credit monitoring services; or
- identity theft insurance.
- Prepare a notification timeline or schedule.

## EXECUTE THE NOTIFICATION PLAN

While specific legal requirements may depend on the facts of the breach, typically, when notifying individuals, an county should:

- Prepare and maintain a list or database of persons to be notified that includes:
  - the person's name and address;
  - other contact and identifying information for the person;

- the affected data elements; and
- the notification status.

- Determine the method of notification, considering that applicable law or contracts may require certain modes of communication.
- Draft template notification letters to affected persons that take into account:
  - the specific content requirements for the notifications, which are typically dictated by statute; and
  - whether the affected person is a minor or is deceased, in which case the letters should be directed to personal representatives or guardians and may differ as to whether and what mitigation products are offered.
- Draft notification letters, if they are required, to:
  - credit reporting agencies; and
  - regulatory or law enforcement agencies.
- Draft substitute notice if permitted or required by law.
- See sample notification letters are attached to this policy.

**POST-NOTIFICATION AND BREACH RESPONSE REVIEW**

- Review applicable access controls, policies, and procedures and determine whether to take any actions to strengthen the county's security program.
- Review the response to determine whether any changes should be made to the county's incident response policy or procedures.

# Security Breach Identification Form

*****In event of breach or suspected breach, Franklin County IT Department is to fill out this form and return it to the Franklin County Risk Manager**

## General Information

**Security Breach Detected By:** Name: Title:

Department/Division:

Phone: Alt. Phone:

E-mail:

Address:

Date and Time Detected:

Location Incident Detected From:

Additional Information:

## Security Breach Summary

**Security Breach Location:**

Site: Site Contact Person:

Phone:

E-mail: Address:

**How was the security breach detected:**

**Describe techniques used to detect the security breach:**

**If security breach is only suspected, please describe why you suspect a security breach has occurred.**

**What Data Elements were compromised?** (Do not provide the raw data just describe the data elements)

**Approximate number of individuals whose data was compromised:**

**Can WA State residents be determined from available data? Yes No**

**Describe what action has been taken so far:**

**Additional Information:**

# Security Breach System Survey Form

*****In event of breach or suspected breach, Franklin County IT Department is to fill out this form and return it to the Franklin County Risk Manager**

**Location(s) of affected systems:**

**Describe affected information system(s):** (one form per system is recommended)

Hardware Manufacturer:

Serial Number: Asset Tag:

**Was the affected system connected to the network? Yes No**

**Is the affected system still connected to the network? Yes No**

System Name:

System IP Address: MAC Address:

**Describe the physical security of the location of affected information systems** (locks, security alarms, building access, etc.):

SAMPLE LETTER 1(on Department letterhead)
Data Acquired: Credit card Number or Financial Account Number

Dear :
I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, what kind of Personal Information was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. We recommend that you immediately contact [*credit card or financial account issuer*] at [*phone number*] and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask [*name of account issuer*] to give you a PIN or password. This will help control access to the account.

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

| Equifax | Experian | Trans Union |
|---|---|---|
| 800-525-6285 | 888-397-3742 | 800-680-7289 |

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for Personal Information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency and applicable case number investigating the incident.*] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft we suggest that you contact the Office of Attorney General. The telephone numbers is (360) 753-6200. Or you can visit their web site at http://www.atg.wa.gov/consumer/idprivacy/IDTheftWhatToDo.shtml. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing – Department Director's Signature*]

SAMPLE LETTER 2 (on Department letterhead)
(Data Acquired: Driver's License or Washington ID Card Number)

Dear :

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, how the drivers license or Washington state identification card was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. Since your Driver's License [*or Washington Identification Card*] number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license.

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

| Equifax | Experian | Trans Union |
|---|---|---|
| 800-525-6285 | 888-397-3742 | 800-680-7289 |

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for Personal Information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency and applicable case number investigating the incident.*] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft we suggest that you contact the Office of Attorney General. The telephone numbers is (360) 753-6200. Or you can visit their web site at http://www.atg.wa.gov/consumer/idprivacy/IDTheftWhatToDo.shtml. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing – Department Director's Signature*]

SAMPLE LETTER 3 (on Department letterhead)

(Data Acquired: Social Security Number)

Dear :

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, how the Social Security Number was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft.

We recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Then call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

| Equifax | Experian | Trans Union |
|---|---|---|
| 800-525-6285 | 888-397-3742 | 800-680-7289 |

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for Personal Information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency and applicable case number investigating the incident.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft we suggest that you contact the Office of Attorney General. The telephone numbers is (360) 753-6200. Or you can visit their web site at http://www.atg.wa.gov/consumer/idprivacy/IDTheftWhatToDo.shtml. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing – Department Director's Signature*]