DATA BREACH RESPONSE

A Guide for Business

Federal Trade Commission | business.ftc.gov

You just learned that your business experienced a data breach. Whether hackers took personal information from your corporate server, an insider stole customer information, or information was inadvertently exposed, you are probably wondering what to do next.

What steps should you take and whom should you contact if personal information may have been exposed? Although the answers vary from case to case, the following guidance from the Federal Trade Commission (FTC) can help you make smart, sound decisions.

This guide addresses the steps to take once a breach has occurred. For advice on implementing a plan to protect consumers' personal information and prevent breaches and unauthorized access, check out the FTC's *Protecting Personal Information: A Guide for Business* (ftc.gov/ProtectingPersonalInformation), and *Start with Security: A Guide for Business* (ftc.gov/StartWithSecurity).

Secure Your Operations

Mobilize your breach response team right away. The exact steps to take depend on the nature of the breach and the structure of your business, but this is the time to implement your existing incident response plan.

Move quickly to secure your systems and fix vulnerabilities that may have caused the breach. The only thing worse than a data breach is multiple data breaches. Take steps so it doesn't happen again.

- **Secure physical areas potentially related to the breach.** Lock them and change access codes, if needed. Ask your forensics experts and law enforcement when it is reasonable to resume regular operations.
- **Stop additional data loss.** Take all affected equipment offline as soon as possible — but don't turn any machines off until the forensic experts arrive. Closely monitor all entry and exit points, especially those involved in the breach. If possible, put clean machines online in place of affected ones. In addition, update credentials and passwords of authorized users. If a hacker stole credentials, your system will remain vulnerable until you change those credentials, even if you've removed the hacker's tools.

Assemble a team of experts to conduct a comprehensive breach response. Depending on the size and nature of your company, your team may include forensics, legal, information security, information technology, operations, human resources, communications, investor relations, and management.

- **Identify a data forensics team.** Consider hiring independent forensic investigators to help you determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps.

- **Consult with legal counsel.** Talk to your legal counsel. Then you may consider hiring outside legal counsel with privacy and data security expertise. They can advise you on federal and state laws that may be implicated by a breach.

Remove improperly exposed information.

- **Your website:** If the data breach involved personal information improperly posted on your website, immediately remove it. Be aware that internet search engines store, or "cache," information for a period of time. You can contact the search engines to ensure they don't archive personal information posted in error.

- **The cloud:** If you inadvertently exposed data stored in the cloud, lock it down.

- **Other websites:** Search for your company's exposed data to make sure no other websites, like archive sites, have saved a copy. If you find any, or if others have received the data, contact those sites and ask them to delete it.

Interview people who discovered the breach. Also, talk with anyone else who may know about it. If you have a customer service center, make sure the staff knows where to forward information that may aid your investigation of the breach. Document your investigation.

Don't destroy evidence. Preserve any forensic evidence during your investigation and remediation.

Fix Vulnerabilities

Think about service providers. If service providers were involved, examine what personal information they can access and decide if you need to change their access privileges. Also, ensure your service providers are taking the necessary steps to make sure another breach doesn't occur. If your service providers say they have remedied vulnerabilities, verify that they really fixed things.

Check your network segmentation. When you set up your network, you likely segmented it so that a breach on one server or in one site could not lead to a breach on another server or site. Work with your forensics experts to analyze whether your segmentation plan was effective in containing the breach. If you need to make any changes, do so now.

Check your code. If a software bug played a part in the breach, ensure that the same or similar bugs don't exist in other software. Review and improve your organization's secure development practices. Consider using bug bounties — rewards to help identify software vulnerabilities.

Work with your forensics experts. Find out if measures such as encryption were enabled when the breach happened. Analyze backup or preserved data. Review logs to determine who had access to the data at the time of the breach. Also, analyze who currently has access, determine whether that access is needed, and restrict access if it isn't. Verify the types of information compromised, the number of people affected, and whether you have contact information for those people. When you get the forensic reports, take the recommended remedial measures as soon as possible.

Have a communications plan. Create a comprehensive plan that reaches all affected audiences — employees, customers, investors, business partners, and other stakeholders. Don't make misleading statements about the breach. And don't withhold key details that might help consumers protect themselves and their information. Also, don't publicly share information that might put consumers at further risk.

Anticipate questions that people will ask. Put top-tier questions and clear, plain-language answers on your website where they are easy to find. Good communication up front can limit customers' concerns and frustration, saving your company time and money later.

Notify Appropriate Parties

When your business experiences a data breach, notify law enforcement, other affected businesses, and affected individuals.

Determine your legal requirements. All states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. In addition, depending on the types of information involved in the breach, there may be other laws or regulations that apply to your situation. Check state and federal laws or regulations for any specific requirements for your business.

Notify law enforcement. Call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police aren't familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service.

For incidents involving mail theft, contact the U.S. Postal Inspection Service.

Did the breach involve electronic personal health records? Check if you're covered by the Health Breach Notification Rule. If so, you must notify the FTC and, in some cases, the media. *Complying with the FTC's Health Breach Notification Rule* explains who you must notify, and when. Also, check if you're covered by the HIPAA Breach Notification Rule. If so, you must notify the Secretary of the U.S. Department of Health and Human Services (HHS) and, in some cases, the media. HHS's Breach Notification Rule explains who you must notify, and when.

Health Breach Resources

HIPAA Breach Notification Rule:

hhs.gov/hipaa/for-professionals/breach-notification

HHS HIPAA Breach Notification Form:

hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting

Complying with the FTC's Health Breach Notification Rule:

ftc.gov/healthbreachnotificationrule

Notify affected businesses. If account access information — say, credit card or bank account numbers — has been stolen from you, but you don't maintain the accounts, notify the institution that does so it can monitor the accounts for fraudulent activity. If you collect or store personal information on behalf of other businesses, notify them of the data breach.

If Social Security numbers have been stolen, contact the major credit bureaus for additional information or advice. If the compromise may involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts and credit freezes for their files.

Equifax: equifax.com/personal/credit-report-services
or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Notify individuals. If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused. In deciding who to notify, and how, consider:

- state laws
- the nature of the compromise
- the type of information taken
- the likelihood of misuse
- the potential damage if the information is misused

For example, thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage.

When notifying individuals, the FTC recommends you:

- **Consult with your law enforcement contact** about the timing of the notification so it doesn't impede the investigation.

- **Designate a point person within your organization for releasing information.** Give the contact person the latest information about the breach, your response, and how individuals should respond.
- **Consider using letters (see sample below), websites, and toll-free numbers** to communicate with people whose information may have been compromised. If you don't have contact information for all of the affected individuals, you can build an extensive public relations campaign into your communications plan, including press releases or other news media notification.
- **Consider offering at least a year of free credit monitoring or other support** such as identity theft protection or identity restoration services, particularly if financial information or Social Security numbers were exposed. When that information is exposed, thieves may use it to open new accounts.

State breach notification laws typically tell you what information you must, or must not, provide in your breach notice. In general, unless your state law says otherwise, you'll want to:

- **Clearly describe what you know about the compromise. Include:**
  - how it happened
  - what information was taken
  - how the thieves have used the information (if you know)
  - what actions you have taken to remedy the situation
  - what actions you are taking to protect individuals, such as offering free credit monitoring services

» how to reach the relevant contacts in your organization

Consult with your law enforcement contact about what information to include so your notice doesn't hamper the investigation.

- **Tell people what steps they can take, given the type of information exposed, and provide relevant contact information.** For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts or credit freezes be placed on their credit reports. See IdentityTheft.gov/databreach for information on appropriate follow-up steps after a compromise, depending on the type of personal information that was exposed. Consider adding this information as an attachment to your breach notification letter, as we've done in the model letter below.

- **Include current information about how to recover from identity theft.** For a list of recovery steps, refer consumers to IdentityTheft.gov.

- **Consider providing information about the law enforcement agency working on the case, if the law enforcement agency agrees that would help.** Identity theft victims often can provide important information to law enforcement.

- **Encourage people who discover that their information has been misused to report it to the FTC, using IdentityTheft.gov.** IdentityTheft.gov will create an individualized recovery plan, based on the type of information exposed. And, each report is entered into the Consumer Sentinel Network, a secure, online database available to civil and criminal law enforcement agencies.

- **Describe how you'll contact consumers in the future.** For example, if you'll contact consumers only by mail, then say so. If you won't ever call them about the breach, tell them that. This information may help victims avoid phishing scams tied to the breach, while also helping to protect your company's reputation. Some organizations tell consumers that updates will be posted on their website. This gives consumers a place they can go at any time to see the latest information.

Model Letter

The following letter is a model for notifying people whose Social Security numbers have been stolen. When Social Security numbers have been stolen, it's important to advise people to place a free fraud alert or credit freeze on their credit files. A fraud alert may hinder identity thieves from getting credit with stolen information because it's a signal to creditors to verify the consumer's identity before opening new accounts or changing existing accounts. A credit freeze stops most access to a consumer's credit report, making it harder for an identity thief to open new accounts in the consumer's name.

[Name of Company/Logo] Date: [Insert Date]

NOTICE OF DATA BREACH

Dear [Insert Name]:
We are contacting you about a data breach that has occurred at [insert Company Name].

What Happened?

[Describe how the data breach happened, the date of the breach, and how the stolen information has been misused (if you know).]

What Information Was Involved?

This incident involved your [describe the type of personal information that may have been exposed due to the breach].

What We Are Doing

[Describe how you are responding to the data breach, including: what actions you've taken to remedy the situation; what steps you are taking to protect individuals whose information has been breached; and what services you are offering (like credit monitoring or identity theft restoration services).]

What You Can Do

The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to verify your identity before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax: equifax.com/personal/credit-report-services or 1-800-685-1111

Experian: experian.com/help or 1-888-397-3742

TransUnion: transunion.com/credit-help or 1-888-909-8872

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's IdentityTheft.gov site to report the identity theft and get recovery steps. Even if you don't find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider placing a free credit freeze. A credit freeze means potential creditors can't get your credit report. That makes it less likely

that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

We have attached information from the FTC's website, IdentityTheft.gov/databreach, about steps you can take to help protect yourself from identity theft. The steps are based on the types of information exposed in this breach.

Other Important Information

[Insert other important information here.]

For More Information

Call [telephone number] or go to [Internet website]. [State how additional information or updates will be shared or where they will be posted.]

[Insert Closing]

[Your Name]

As noted earlier, we suggest that you include advice tailored to the types of personal information exposed. The example below is for a data breach involving Social Security numbers. This advice and advice for other types of personal information is available at IdentityTheft.gov/databreach.

Optional Attachment

FEDERAL TRADE COMMISSION
IdentityTheft.gov

What information was lost or exposed?

Social Security number

- ☐ If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- ☐ Get your free credit reports from AnnualCreditReport.com. Check for any accounts or charges you don't recognize.
- ☐ Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.
  - If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone — or any service that requires a credit check.
  - If you decide not to place a credit freeze, at least consider placing a fraud alert.
- ☐ Try to file your taxes early — before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
- ☐ Don't believe anyone who calls and says you'll be arrested unless you pay for taxes or a debt — even if they have part or all of your Social Security number, or they say they're from the IRS.
- ☐ Continue to check your credit reports at AnnualCreditReport.com. You can order a free report from each of the three credit reporting companies once a year.

For More Guidance From the FTC

This publication provides general guidance for an organization that has experienced a data breach. If you'd like more individualized guidance, you may contact the FTC at 1-877-ID-THEFT (877-438-4338). Please provide information about what has occurred, including the type of information taken, the number of people potentially affected, your contact information, and contact information for the law enforcement agent with whom you are working. The FTC can prepare its Consumer Response Center for calls from the people affected, help law enforcement with information from its national database of reports, and provide you with additional guidance as necessary. Because the FTC has a law enforcement role with respect to information privacy, you may seek guidance anonymously.

For more information and resources, visit business.ftc.gov.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

Federal Trade Commission
business.ftc.gov
August 2023