DATA BREACH RESPONSE:

Best Practices for Small Businesses

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 on your company's website, 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 you take once a breach has occurred. For advice on implementing a plan to protect consumers' personal information, to prevent breaches and unauthorized access, check out the FTC's *Protecting Personal Information: A Guide for Business* and *Start with Security*: *A Guide for Business.*

FIX VULNERABILITIES

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.

Mobilize your breach response team right away to prevent additional data loss. The exact steps to take depend on the nature of the breach and the structure of your business.

IMMEDIATE STEPS

Assemble a team of experts to conduct a comprehensive breach response. Depending on the size and nature of your company, they 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 and breach response experience. They can advise you on federal and state laws and recommend response and remediation procedures.

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 immediately—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.

Remove improperly posted information from the web.

- 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 that they don't archive personal information posted in error.
- Other websites: Search for your company's exposed data to make sure that no other websites have saved a copy. If you find any, contact those sites and ask them to remove 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.

Do not destroy evidence. Don't destroy any forensic evidence in the course of your investigation and remediation.

NEXT STEPS

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 does not 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.

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 is not. 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.

Then, put top tier questions in 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.

Send Notification

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

Determine your Legal Requirements

Most 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 Health Information?

Then 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 names and 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 or 1-800-525-6285

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

TransUnion: transunion.com or 1-800-680-7289

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 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, 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 notifications.

- 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 such information is exposed, thieves may use it to open new accounts.

Most states have breach notification laws that 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 and contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. 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 on page 10.
- 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 file a complaint with the FTC, using identitytheft.gov. This information 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 only contact consumers by mail, then say so. If you won't ever call them about the breach, then let them know. This information may help victims avoiding 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 names and 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 on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it's a signal to creditors to contact the consumer before opening new accounts or changing existing accounts.

Also, advise consumers to consider placing a credit freeze on their file. The cost to place and lift a freeze depends on state law.

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

NOTICE OF A 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

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call 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 90 days. You can renew it after 90 days.

Equifax: equifax.com or 1-800-525-6285

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

TransUnion: transunion.com or 1-800-680-7289

Request that all three credit reports be sent to you, free of charge, for your review. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and call [insert contact information for law enforcement if authorized to do so]. Get a copy of the police report; you may need it to clear up the fraudulent debts.

If your personal information has been misused, visit the FTC's site and identitytheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

You also may want to consider contacting the major credit bureaus at the telephone numbers above to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. Find your state Attorney General's office at naag.org to learn more.

We have enclosed a copy of *Identity Theft: A Recovery Plan*, a comprehensive guide from the FTC to help you guard against and deal with identity theft. We've also attached information from IdentityTheft.gov about steps you can take to help protect yourself from identity theft, depending on the type of information exposed.

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]

Consider attaching the relevant section from identityTheft.gov, based on the type of information exposed in the breach. This is for a data breach involving Social Security numbers. There is similar information about other types of personal information.