American Bank Systems-Data Breach-Frequently Asked Questions

1. Is this letter a scam?

No. The letter is legitimate and contains background information on the incident and the resources available to you. ABS has set up a dedicated call center to answer all your questions and you can contact this call center with confidence. **ABS hotline 855-914-4705 (open 9:00 AM to 9:00 PM EST)**

2. What happened and why was my information in their system?

American Bank Systems ("ABS") is a vendor of InFirst Bank. They provide electronic administration software services to their bank partners. Your information was on their system as part of this service. Many banks utilize these types of vendor services. They became aware that they were victimized by a cybercriminal and certain systems were infected with malware. ABS's investigation first determined that information related to certain bank customers was part of the information affected. InFirst Bank was notified on November 18, 2020 and began working with ABS to finalize a customer mailing list. ABS has no evidence of any identity theft or fraud connected to this event but provided notice on behalf of InFirst Bank in an abundance of caution.

3. What information was impacted?

We have been notified by ABS that the data potentially affected was names, addresses, social security numbers, and dates of birth, as well as, bank account numbers.

4. Do I need to open a new checking account?

We believe there is very little risk at all associated with your account number. Consider that every time you give someone a check they have your name, address, and account number. Your checking account and debit card have the same protections against unauthorized transactions as they currently do. Just as is the current practice, if you see any unusual activity then report it immediately and we will work through it with you and provide resolution.

5. Has my information been misused?

At this time, there is no indication of identity theft or fraud as a result of this incident. However, we encourage all individuals, as a general practice, to protect against the possibility of identity theft and fraud.

6. What can I do to protect against identity theft or fraud?

You can do any of the following to protect against identity theft or fraud: **(Contact information is available at the end of the FAQ's or refer to the "Steps you can take to protect your information" insert provided in your letter.)**

- **Credit Report Monitoring:**
  - Take advantage of the offer by ABS to provide 12-months of free credit report monitoring as outlined in your letter. You should monitor your credit report regardless of whether your information has been exposed or you think you may be a victim of identity theft or fraud.
  - Also, every U.S. consumer over the age of eighteen can receive one free credit report every twelve months by contacting one of the three national credit bureaus or through the Annual Credit Report Service.
- **Monitoring your financial statements carefully**. If you see any unauthorized or suspicious activity, promptly contact the bank.
- **Monitoring your credit reports for suspicious or unauthorized activity**. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. You may also contact the three major credit bureaus directly to request a free copy of your credit report. That contact information was provided in your letter and is available following these FAQ's.
- **Fraud alerts: Placing a fraud alert on your credit file**. You have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. A fraud alert tells creditors to contact you before they open a new credit account under your Social Security number. A business is required to take steps to verify the consumer's identity before

extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Contact the three major credit bureaus directly to place a fraud alert on your credit file. The contact information was provided in your letter and is available following these FAQ's.

- **Security Freeze: Considering a security freeze on your credit file**. A security freeze should be given much thought before applying this to your credit. While it will keep any fraudulent credit from being established it will also prevent you from applying for credit if you forget to remove the security freeze first. This type of freeze will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Contact the three major credit bureaus directly to place a security freeze on your credit file. The contact information was provided in your letter, or I can email the information to you.
- **Contacting the Federal Trade Commission and your state Attorney General** to learn more about identity theft, fraud alerts, security freezes, and other steps you can take to protect yourself.
- **Reporting incidents of suspected or actual identity theft or fraud** to law enforcement, the Federal Trade Commission, and the state Attorney General.

7. I am a business. Will I have credit monitoring?
A business EIN number does not qualify for credit monitoring, however, if you have personal accounts you should have also received an individual letter and WILL be eligible for the credit monitoring offer for yourself personally.

8. What is ABS doing in response to this incident?
In addition to conducting an investigation, ABS took steps to further strengthen the security of its systems, including resetting passwords and implementing advanced endpoint monitoring. ABS also notified federal law enforcement regarding this incident.

9. There are fraudulent charges on my credit/debit card. What do I do?
We will dispute any reported fraudulent charges the same way we currently do. Depending on our investigation results and the type of fraud, you may need to report incidents of identity theft to the local law enforcement agency, the Federal Trade Commission, and the state Attorney General.

10. What is the purpose of a "fraud alert"?
A fraud alert tells creditors to take additional steps to verify your identity and/or contact you before they open a new credit account under your Social Security number.

11. What is the purpose of a security freeze?
A security freeze will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

12. I think I may be a victim of identity theft. What should I do?
If you believe you are a victim of attempted or actual identity theft or fraud, we encourage you to take the following steps:

- Contact any financial institution to make them aware and protect or close any accounts that have been tampered with or opened fraudulently.
- Contact the credit reporting agencies to place a "fraud alert" or a "credit freeze" on reports.
- File a police report and ask for a copy for your records.
- File a complaint with the Federal Trade Commission
- File a complaint with the state attorney general.
- Keep good records.
    - Keep notes of anyone you talk to regarding this incident, what s/he told you, and the date of the conversation;
    - Keep originals of all correspondence or forms relating to the suspicious activity, identity theft, or fraud; and
    - Retain originals of supporting documentation, such as police reports and letters to and from creditors; send copies only and keep old files, even if you believe the problem is resolved.

13. I heard about this from another source; am I impacted by this incident?
If you did not receive a letter then you were not identified as someone who was potentially affected.

14. Why did it take so long to notify me?
Upon learning of the malware attack, ABS immediately launched an investigation to determine the nature and scope of this event. This included working with third-party computer forensic specialists to determine the exact information impacted by the event. ABS worked as quickly as possible to provide notice of this incident following completion of the investigation.

15. The letter was sent to a deceased individual. Do I need to do anything?
We encourage you to remain vigilant, to review your loved one's account statements regularly, and to monitor your loved one's credit reports for suspicious activity. In addition, there are steps you can take to protect your loved one's credit file. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus so long as you verify your authorization to make such a request on behalf of your loved one. You may also contact the three major credit bureaus directly to request a free copy of this credit report. We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

You may also request, in writing, that the report list the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate—noting the relationship of any individual listed to your family member—and/or a law enforcement agency)."

In most cases, this flag will prevent the opening of new credit accounts in your loved one's name.

16. The letter was sent to my minor child. Do I need to do anything?
If you visit the https://www.transunion.com/ website there is extensive information on what you can do for a minor. You can type "child" in the search bar or click on Credit Help>Credit Freeze, and there are options for **"Freeze a Loved Ones Credit"**.

REFERENCE INFORMATION:

- **ABS HOTLINE: 855-914-4705 (open 9:00 am to 9:00 pm EST)**
- **THREE MAJOR CREDIT BUREAUS:**

Equifax	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
https://www.equifax.com/personal/	https://www.experian.com/	https://www.transunion.com/

- **FREE ANNUAL CREDIT REPORTS:**
  Every U.S. consumer over the age of eighteen can receive one free credit report every twelve months by contacting one of the three national credit bureaus or through the Annual Credit Report Service by visiting www.annualcreditreport.com or calling toll-free, 1-877-322-8228. **TIP:** They can pull one credit report every 4 months and monitor all year.

- **FEDERAL TRADE COMMISION:**
  To file a complaint with the FTC, or to obtain additional information on identity theft and the steps that can be taken to avoid identity theft, the FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580, or at www.ftc.gov/idtheft, or (877) ID-THEFT (877-438-4338); TTY: (866) 653-4261.

- **PA STATE ATTORNEY GENERAL:**
  Josh Shapiro-Consumer Protection- 800-441-2555
  https://www.attorneygeneral.gov/get-help/