September 2024

CLIENT BULLETIN: ESSENTIAL STEPS TO SAFEGUARD PERSONAL INFORMATION POST-BREACH

In August 2024, the hacker known as USDoD claimed responsibility for one of the largest data breaches in history, affecting nearly 2.9 billion individuals. The breach targeted National Public Data (NPD), a company that specializes in background checks and exposed highly sensitive personal information, including social security numbers, full names, addresses, dates of birth, and phone numbers.

Allied Solutions' risk mitigation experts are answering some top-of-mind questions about how to support your accountholders in the wake of this unprecedented breach.

Q: Who is USDoD?
A: USDoD (previously known as NetSec) is believed to be a single person operating out of a country that does not prosecute for cybercrimes against some countries. The hacker has garnered significant attention due to the scale of their recent exploits. Despite their provocative name, which likely alludes to the U.S. Department of Defense, little is known about their actual location or the hacker's identity.

Q. What happens to the stolen data?
A: The stolen data was posted on a dark web bulletin board, which was made available for download to anyone with access to it. Once in possession of the stolen data, groups and individuals like USDoD typically engage in a variety of activities to monetize the information, including selling it again on the dark web, committing identity theft, launching phishing attacks, and even extortion.

Q. How does an individual know if their information was compromised?
A: The researchers at Pentester.com have created a website to help people determine if their personal information was part of the NPD breach. This tool allows you to enter your details and quickly check if your data has been exposed. (Young children and elderly adults are not exempt from the risk. Their information could be exploited.) While not foolproof, it's a useful resource to assess whether you need to take further action. Visit the website here to validate if your information was compromised.

Q. What resources are available to continue to mitigate risk?
A. Allied is committed to providing educational resources to financial institutions. Download the free checklist, Managing the Impact of a Large-Scale Data Breach.

Q. Should our FI still use SSNs as a form of authentication and verification?
A. It is no longer considered best practice to rely solely on social security numbers as a sole form of authentication. Historically, SSNs were considered private (not-publicly-available) but this breach reinforces the importance of multi-factor authentication.

Help Your Accountholders Safeguard Their Identity

This data breach is both large-scale and severe. It is crucial to take immediate steps to educate accountholders in protecting their identity. Share these eight protective measures with your accountholders as soon as possible.

8 Ways to Protect Your Identity After the Social Security Number Breach:

1. **Freeze credit with all 3 bureaus:** Place a credit freeze with all three major credit bureaus—Equifax, Experian, and TransUnion. A credit freeze restricts access to your credit report, making it difficult for identity thieves to open new accounts in your name. You can lift the freeze temporarily if you need to apply for credit. To prevent a malicious actor from using the stolen data, set up online accounts with each bureau to prevent malicious actors from setting up an account on your behalf.

2. **Enable fraud alerts:** Use this resource to search your name, state and date of birth to see if your information may have been included in the breach. Place a fraud alert on your credit file with each of the three credit bureaus.

3. **Review credit reports:** Obtain free copies of your credit reports from Equifax, Experian, and TransUnion via AnnualCreditReport.com. Review the reports a few times a year for any inaccuracies or unfamiliar accounts and dispute any errors with the credit bureaus.

4. **Be vigilant against phishing:** Be cautious when receiving unsolicited emails, texts, or phone calls asking for personal information, even ones that *seem* legitimate. Cybercriminals use creative, convincing phishing tactics to trick you into revealing sensitive details. Remember, phone numbers were also included in this breach.

5. **Monitor all financial accounts:** Regularly review your bank statements, credit card accounts, and other financial transactions for any unauthorized activity. Set up alerts with your bank and credit card companies to receive notifications of unusual charges.

6. **Activate two-factor authentication:** Enable two-factor authentication (2FA) on your financial accounts and other sensitive online services. This adds an extra layer of security by requiring a second form of verification, such as a code sent to your phone, in addition to your password.

7. **Set up your online accounts:** Secure and monitor your government-related online accounts with these sites:
    - login.gov
    - id.me
    - irs.gov
    - ssa.gov

    These accounts provide secure access to important government services and help protect your personal information from unauthorized use.

8. **Consider identity theft protection services:** Identity theft protection services offer comprehensive monitoring and alerts for suspicious activity, as well as assistance in restoring your identity if it is compromised.

By encouraging accountholders to take these proactive measures, your institution can help significantly reduce the impact of the NPD breach. While it is impossible to eliminate the threat, these steps provide a strong defense against the misuse of personal information.

For more risk management and cybersecurity resources for financial institutions, visit our Resource Center.