Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

October 2024

Data breaches: How consumers can respond to help prevent identity theft

A data breach occurs when sensitive information is exposed to unauthorized parties. When this happens, the affected company typically notifies those whose data has been compromised, often via a letter or an email message. In some cases, such notification is legally required.

Be sure to read all notifications thoroughly. Various actions are necessary based on the type of data compromised. Even if seemingly unimportant information is exposed in the breach, scammers can use it to their advantage. When a database with emergency contact information is breached, for example, scammers may use that data to lend credibility to their schemes.

Types of exposed data and consumer responses:

Social Security number

- If the company that is the source of the data breach provides free credit monitoring, consider taking advantage of that offer. These services often include alerts for new credit accounts, dark-web monitoring and identity theft insurance.
- Visit www.AnnualCreditReport.com for free credit reports, available once a week.
- Consider a credit freeze, which locks your credit, preventing new creditors from accessing your reports. This helps shield you from unauthorized accounts being opened in your name. Note that a credit freeze doesn't stop unauthorized charges on existing accounts, so it's crucial to review your statements closely. Contact all three major credit-reporting agencies to initiate a freeze:
    - Experian: www.experian.com – 888-397-3742
    - Equifax: www.equifax.com – 800-525-6285
    - TransUnion: www.transunion.com – 800-680-7289.

Online login or password

- Log in to that account and immediately change your username and password. If you can't log in, contact the company to find out how you can recover or shut down the account.
- If you use the same password anywhere else, change it for the other accounts.
- Is your credit-card number stored in that account? Check your credit-card account for any charges that you don't recognize.
- Use multifactor authentication for your accounts, which adds an extra security layer by requiring an additional step – such as a text to your phone, for access.

Bank-account or credit-card/debit-card information

- If your bank information was exposed, contact your bank to close the account and open a new one. If credit-card or debit-card information was exposed, contact your bank or credit-card company to cancel your card and request a new one. If you contact your credit-card company within two billing cycles, you are generally limited to $50 in liability, which may be waived by your credit-card company. With a debit card, if you report the incident within two business days after discovering the loss, you are liable for up to $50. After two business days, you might be liable for more.
- Examine all bank accounts and payment methods linked to the breach, including credit cards and services such as Venmo and Zelle.

Consumers who suspect an unfair business practice or want help in addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Four steps to being safer in cyberspace

October is Cybersecurity Awareness Month, with the theme this year of "Secure Our World." The Ohio Attorney General's Office is proud to support this annual awareness effort by promoting four steps to improved security in cyberspace when using smartphones, tablets, computers and other internet-connected devices.

1. **Multifactor authentication (MFA):** MFA is already available on many of your online accounts, apps and programs. It adds an extra layer of security by requiring you to verify your identity in addition to entering your

password, usually by sending a code to your mobile device via an email or text message. To authenticate your identity, some MFA systems use biometrics such as facial recognition or a fingerprint. Activating MFA on as many accounts as possible can significantly reduce the risk of unauthorized access. To enable it, check the Account Settings, Privacy or a similar option on your accounts.

2. **Passwords**: Strong, unique passwords are essential for securing your accounts. Experts recommend using passwords of at least 16 characters – including random combinations of letters, numbers and symbols – and ensuring that you have a unique password for *every* account.

To manage multiple passwords, consider using a reputable password manager, which securely stores your passwords and allows you to access them across devices. With a password manager, you need to remember only your master password.

3. **Software updates:** Make sure that your online devices have the latest program updates, paying special attention to anti-virus programs and internet browsers. Be on the lookout for notifications about available updates and install those updates as soon as possible. Activating automatic updates whenever offered saves you from having to remember to check for updates.

4. **Phishing:** Phishing scams are messages designed to appear to come from a trusted source, such as your bank or credit-card company. Phishing occurs when someone impersonates a legitimate person, business or organization to try to trick victims into revealing private data, typically by luring them to click on a malicious link that leads to a phony website. You can spot phishing attempts by recognizing signs, such as the use of language suggesting that the request is urgent and asking you for financial or other personal information. If a message appears suspicious, don't click on any links, download any attachments or call any phone numbers included in the request. Report it to the real organization that is being impersonated or to your email provider – and delete the message. If you need to contact an organization to verify a message, contact the organization using information found on its official website or another legitimate source, such as on the back of your bank debit card or on your credit-card statement.

For more information about National Cybersecurity Awareness Month, visit the National Cybersecurity Alliance website at www.staysafeonline.org. For more cybersecurity tips from the Attorney General's Consumer Protection Section, click here.

Important tips for planning holiday travel

If you're planning to travel this upcoming holiday season, here's some helpful information related to flights, hotels, car rentals and traveler's insurance.

- **Airline flight delays and cancellations:** In April 2024, the U.S. Department of Transportation rolled out new rules that require automatic cash refunds to passengers who experience significantly delayed flights or flight cancellations. The rules took effect on Oct. 1, 2024, with compensation available for delays exceeding three hours for domestic flights and six hours for international flights.
- **Hotel fees:** Many hotels tack on extra fees (such as a "resort fee" or an "amenity fee") which may not be clearly disclosed during the booking process. Be aware of such hidden costs and be sure to consider them when comparing hotel rates.
- **Rental-car insurance and rights:** Rental-car companies often offer additional insurance options for a fee. Be sure to check whether you're already covered by your existing auto or homeowner's insurance,

or, if you're a business traveler, through a business policy. Some credit cards also provide rental insurance or a collision damage waiver when the card is used to pay for the rental.

If a rental-car company doesn't have the vehicle you reserved (no SUVs available, for example), ask the company to check another location or with a competitor for a comparable vehicle. This is generally standard industry practice.

- **Travel insurance:** Travel insurance can provide coverage for unexpected disruptions or accidents, but it typically costs 4-10% of the total trip price. Before purchasing travel insurance, check whether your credit card offers travel-related benefits. If not, shop around and compare policies to ensure you get the coverage you need at the best rate.

Planning ahead and knowing your rights can help ensure a smooth and enjoyable holiday travel experience. Safe travels!

Consumers who suspect a scam or an unfair business practice should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Online shopping: Know the seller

If you're shopping online this holiday season, it's essential to know who's selling the product you're buying. Some companies sell their products directly; others sell from a third party. Websites can sell you products in three ways:

- **Sold and shipped by the website**: The product you purchase is sold and shipped by the website from which you buy it. If you're on a company's website and the product is sold and shipped by the company, your purchase should be covered under the company's return policy.

- **Sold by third party, shipped by website**: The product you buy is sold by a third-party company but shipped by the website from which you buy it. In this case, check the return policy of the website as it relates to third-party sellers. A product not sold and shipped by the seller might have a different return policy.

- **Sold and shipped by a third party**: This means that a product comes directly from the third-party seller, even though the item is advertised on a website that hosts multiple sellers (such as Target, Walmart or Amazon). In such cases, the only interaction this product has with the manufacturer's website is for processing the payment. Check the return policy of both the host website and third-party seller, as they may differ and the host website may not accept direct returns.

Tip: Knowing the origin of the items you're buying can influence your purchase decision. The product description or checkout area should list the brand name, seller and shipper. For example:

- **Brand**: Topps Cards
- **Sold by**: Joe's Trading Cards
- **Fulfilled/Shipped by**: Amazon

The Attorney General's Office offers the following tips for smart online shopping:

- **Plan before you shop**. Carefully review ads and compare deals. Keep an eye out for important exclusions and limitations that must be disclosed in ads, even online. Check the details to see whether

limited quantities of an item are available for sale, the sale price is valid during certain hours only, or other terms and conditions apply.

- **Research online reviews**. Be cautious about reviews posted with generic names and profiles without photos; they might be impersonating legitimate shoppers. Cross-reference customer reviews of the same products on different websites. Consistent reviews on several online stores can add validity to the feedback.
- **Check return policies**. In Ohio, sellers can set their own return policies, including policies of "no returns." But if a policy limits your ability to obtain a refund, a seller must clearly notify you of that policy before you complete the purchase. Also, be sure to check return policies, as they might change during the holiday season.
- **Compare gift cards**. Not all gift cards are alike, so review the terms and conditions before you buy. In general, most gift cards must last at least five years, but fees might vary depending on the type of card, such as a single-store card or a prepaid network-branded card that can be used almost anywhere. Also, promotional cards such as those included free with a purchase might not have the same protections.
- **Check delivery dates and fees**. Carefully review the expected delivery date and shipping costs before making a purchase. Find out whether you'll be charged fees for return shipping or restocking if you return the product. Also, pick up delivered packages promptly to prevent theft or damage outside your door.
- **Beware of package-tracking scams.** A package-tracking scam might involve an email alert, which informs you of a "delay" in the shipping of a package. The email either asks you to provide personal information or to click on a link for additional information. But providing personal information could lead to financial harm, and clicking on the included link could infect your computer with malware. In addition to keeping your shipping confirmation email, keep track of the retailers from which you've ordered. And don't click on links if you're unsure whether the sender is legitimate.
- **Monitor your accounts**. Regularly check your credit-card and bank accounts for unauthorized charges or unexpected activity. If you find problems, immediately notify your credit-card provider or bank. The sooner you identify a problem, the sooner you can work to correct it.

Consumers who suspect an unfair business practice or want help addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

BONUS TIP YOU CAN USE: Are you concerned about changes being made to your house title without your permission? Some of Ohio's county auditors have important and free e-alert programs that will notify you if your property record changes hands.