



Investigator Insights

Breaches Happen.

What You Can Do To Protect Your Personal Information

According to the Identity Theft Resource Center, there have been more than 1,000 data breaches reported this year. You trust the organizations you do business with to protect your personal information, and 80 percent of surveyed executives say their company has developed policies and procedures to mitigate security risks.¹ However, hackers are smart and they can move quickly. They also exploit employees' willingness to trust that an email from an executive or third-party vendor is legitimate, unlocking a treasure trove of valuable information and putting customers at risk of fraud and identity theft.

When you hear of a major breach, your first thoughts are about how you might be affected. This is only natural and there is no way to predict when a breach may happen. However, there are ongoing, proactive steps you can take to protect your information, and help you quickly recognize when you may be at risk.

- **Limit your information sharing.** If someone asks for your Social Security number, ask them why they need it, how they secure records, and what happens if you don't provide it. Don't include your full name, birth date, email address and mobile phone number on public social media profiles.
- **When in doubt, don't click.** Think twice before clicking on a link in any email or text message. Even if the message appears to be from someone you know and trust, hackers have gotten very good at making phishing attempts look legitimate.

- **Check online banking and credit accounts regularly.** You can quickly detect fraudulent charges or notice suspicious activity.
- **Don't ignore snail mail.** Did you receive a credit card for which you didn't apply? A collection notice for an account you don't have? These are identity theft red flags. Also, review Explanation of Benefits (EOB) statements from your medical insurance provider to verify that the listed services/products were received by you or a family member covered by your plan.
- **Check your credit reports.** Ongoing credit monitoring will alert you when something new is reported to the credit bureau file that it is monitoring. However, credit reports should still be reviewed at least annually. Visit annualcreditreport.com or call the Annual Credit Report Request Service at 877-322-8228 to get credit reports from all three reporting bureaus at no cost.
- **Review your Social Security Earnings and Benefits Statement.** Look for errors in your annual income. A difference in what is recorded and what you actually earned could be a sign of employment-related identity theft. To order a statement, call 800.772.1213 or go to ssa.gov.

Think Twice about Freezing Your Credit

Credit freezes become a popular recommendation after a major breach, but Kroll Investigators advise placing a fraud alert with the credit reporting agencies instead. If you are considering a credit freeze, it's important

to understand what a credit freeze is, as well as the benefits and limitations.

A freeze blocks access to your credit file so only the creditors and other businesses with whom you have a current relationship will have access to your reports (with certain exceptions). With a freeze in place on all three of the national credit reporting agency (CRA) reports, new creditors, lenders, landlords, insurance companies, cell phone and utility companies, and potential employers will be unable to evaluate your credit history. Without access to your credit history, any application for credit or other services while the freeze is in place will likely be denied.

Benefits of a credit freeze include:

- Minimizing the risk of credit identity theft.
- If you are already a victim of identity theft, there is usually no charge to place, temporarily lift, or remove a freeze.
- A credit freeze does not affect your credit score.
- In most states, the freeze will remain in effect permanently unless a request is received from the consumer to temporarily lift or permanently remove it. In a small number of states the freeze expires after 7 years.

Limitations include:

- In order to be effective, a freeze must be placed with each of the three credit reporting agencies.
- There can be a fee to place a freeze unless you are a proven victim of identity theft.
- A freeze does not prevent fraud involving existing bank or credit accounts.
- A freeze does not reduce the chance of existing account takeover, nor help prevent non-credit-related issues, such as medical or criminal identity theft, or employment and tax fraud.
- A freeze may not be effective with creditors, including payday loan companies and utilities, who do not run a credit check with the bureaus.

- You must temporarily lift (or “thaw”) the freeze when you want your credit report to be available when applying for credit with a new creditor, potential employer, etc.
- Fees to place and lift freezes, as well as the length of time a freeze is in place, will vary by state.
- Credit bureaus have up to five days to place a freeze after receiving a written request. Your information may still be at risk during this time.
- Credit bureaus have up to three business days to lift a credit freeze; this may be an issue if credit is needed immediately. Currently a few states such as Delaware and New Jersey have passed laws requiring the freeze to be lifted within 15 minutes of the request.
- Each credit bureau requires a separate PIN to lift a credit freeze. If you lose your PINs, you will have to write to each CRA and provide proof of your identification to request a replacement PIN. A fee may be required in some states to replace the PIN.

Breaches can happen to any organization. That’s why it’s important for consumers to be vigilant about protecting their own information.

As an IDShield member, you have already taken one of the most important steps towards protecting your identity in the event of a data breach. As part of your IDShield services, you have unlimited consultation with experienced Kroll Investigators who can help determine if your information has been used fraudulently; and if it has, help you to restore your identity to pre-event status. Call us at 888.494.8519 with any questions or concerns you may have.

¹Global Fraud & Risk Report, Annual Edition 2016/17, Kroll

