RCM&D

Assurex GLOBAL | Private Client Practice Group

Identity Fraud

Taking the Necessary Steps to Prevent this Common Crime

IN 2015 ALONE, OVER 13 MILLION AMERICANS fell victim to identity fraud, resulting in damages of more than $15 billion. While it is impossible to prevent fraud entirely (your data is often in the hands of others—banks, hospitals, online stores, etc.), there are steps you can take to lower the risk of exposure.

In addition to prevention, it is equally important to be aware of the options you have available to resolve an identity fraud incident should it ever happen to you.

To help our associates, Partners, and clients protect against identify fraud, Assurex Global asked our "go-to" resource for digital forensics and cybersecurity, LIFARS, for advice. What follows is a sampling of questions it commonly hears from clients, and its advice for preventing identity fraud and taking action should your identity become compromised.

Who are the criminals behind identity theft?

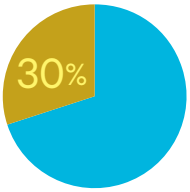
Unknown hackers automate the majority of attacks. However, it's important to remember that 30 percent of identity fraud is committed by a person we know. To protect yourself from those who may be close to you:

- Restrict access to your Personally Identifiable Information (PII)
- Avoid sharing access to personal devices like laptops and mobile phones/tablets
- Secure documents like birth certificates, Social Security cards, insurance policies and health records in a deposit box outside of your residence

How can I secure my online presence from identity theft?

It's recommended to follow basic security and privacy hygiene. This includes using strong passwords, securing your laptop, mobile devices, and home Wi-Fi network, and not using public Wi-Fi networks for matters requiring exchanges of PII, payments, passwords, etc.

For a more complete list of cybersecurity best practices to help raise your overall level of personal protection, please refer to our previous LIFARS updates on Online Privacy, Cybersecurity Security, and Cybersecurity while Traveling.



30% of identity fraud is committed by a person we know

MAY 2016
ASSUREX GLOBAL QUARTERLY SECURITY UPDATED PROVIDED IN COLLABORATION WITH LIFARS

Should I monitor my credit to prevent fraud?

No. Experts agree that credit monitoring may not be the best way to monitor your credit file and prevent fraud. Instead, it's recommended to take advantage of a Credit Freeze and Fraud Alerts—both of which are designed to prevent fraud.

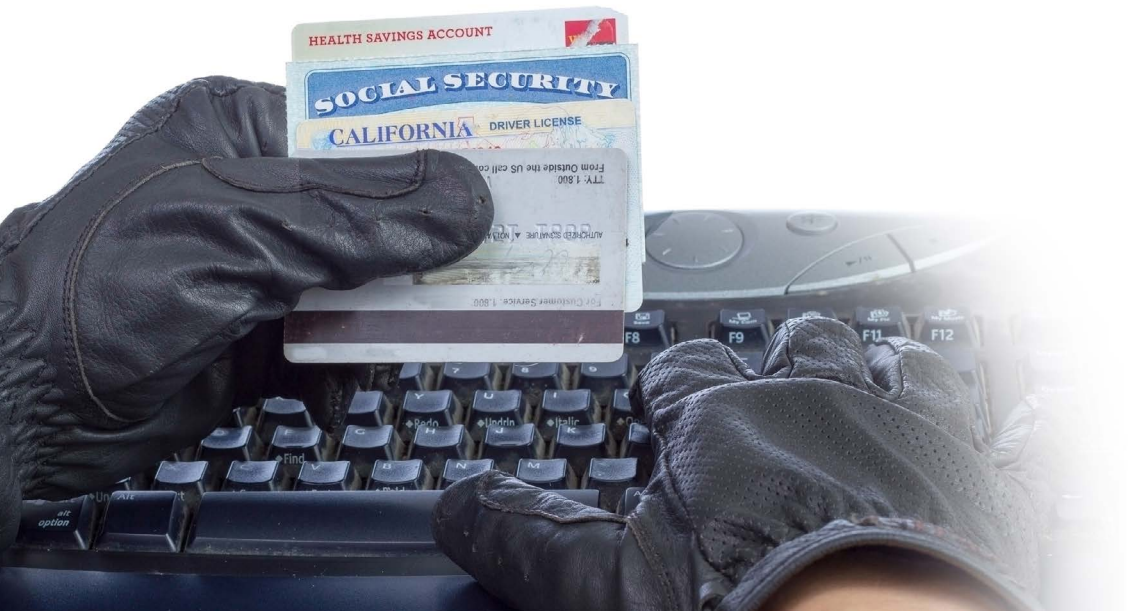
A Credit Freeze prevents the opening of new credit lines and "freezes" your credit file. This tactic will prevent any access to your credit files, even for background checks. To open a new line, the account needs to be "thawed."

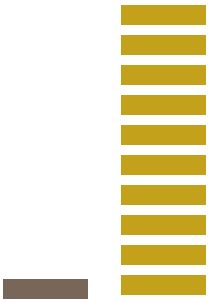
Fraud Alerts will notify you if there are new lines of credit opened in your name. They will also request the credit issuer to verify the applicant prior to opening the account. They are available in 90 day or 7 year increments.

A company notified me that their data has been breached—what should I do?

Data breach notifications must be taken seriously; statistically, victims of a breach are 10 times more likely to have their identity stolen than non-victims. In most cases, the criminals do not get the complete set of information needed to commit fraud, and they often use phishing campaigns—by email or by phone—to obtain the missing information.

If you are a victim of a data breach, remain vigilant and scrutinize every email and phone call relating to the breach. If you're unsure of a communication's authenticity, call the company in question at the number provided on their website. If available, opt-in to any free notifications.





Victims of a breach are 10 times more likely to have their identity stolen than non-victims.

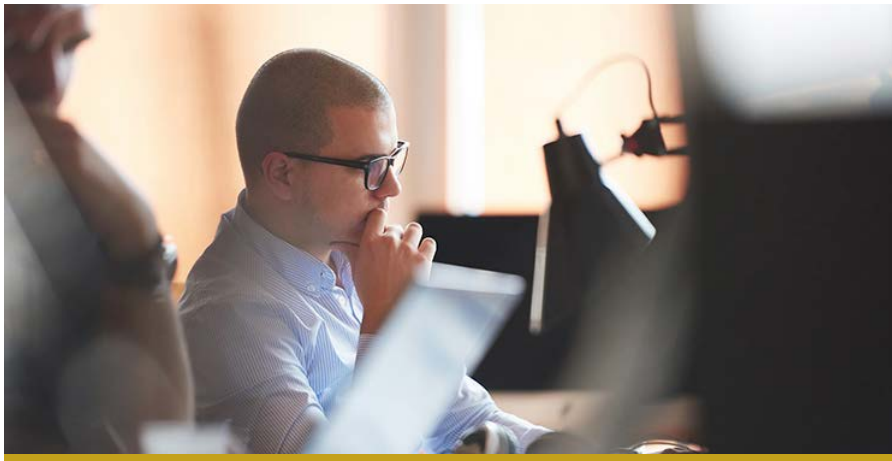
What should I do if I become the victim of identity theft?

Take immediate action. Immediately contact the institution involved—e.g. if your credit card was stolen, call your bank. Then, file a police report and an Identity Theft Affidavit with the Federal Trade Commission (FTC) to create an Identity Theft Report. The Identity Theft Report is needed for easier communication with the credit reporting agencies. The FTC and police will advise you on next steps for your particular case.

Review your accounts. Monitoring accounts potentially involved in the identity theft or data breach will help detect suspicious activity and prevent the criminals from further damaging your credit score or stealing money from you. Review your credit reports for unauthorized accounts opened in your name. In most cases, it's advised to close and re-open accounts as a preventive measure—even on accounts seemingly not involved.

Take preventive steps. Now is a good time for the best practices mentioned above—a Credit Freeze and Fraud Alerts.

Be proactive. You can take action even if no direct evidence of fraud has been observed. For example, if the identity theft included your Social Security Number, you need to contact the Social Security Administration. The fraud may occur at a later time.



RCM&D

RCM&D is ranked among the top independent insurance advisory firms in the United States. Our specialized teams provide strategic solutions and consulting for risk management, insurance and employee benefits. Leveraging 130 years of experience and strong local, national and global reach, we partner with you to meet all of your business objectives.

LIFARS
your digital world, secured

LIFARS is a digital forensics and cybersecurity intelligence firm based in New York City. Our incident response and penetration testing teams consist of the top experts in the field. As a testament to our excellence, LIFARS was ranked the #2 cybersecurity company in New York Metro area on the Cybersecurity 500 list of the hottest and most innovative cyber security companies.

MAY 2016
ASSUREX GLOBAL QUARTERLY
SECURITY UPDATED PROVIDED
IN COLLABORATION WITH LIFARS