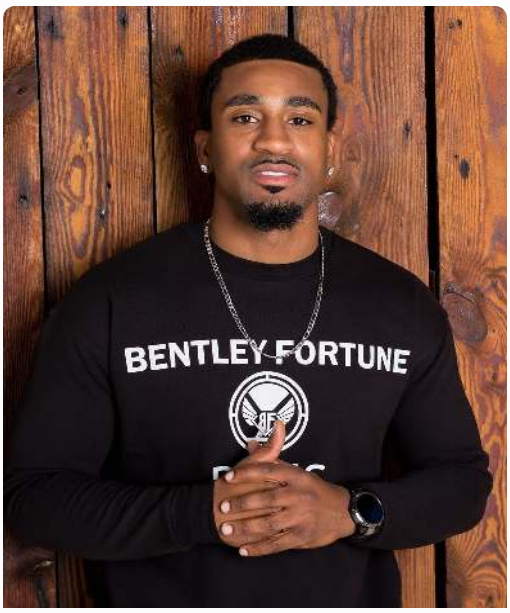
What to Do If You Have Been Defrauded?

ALLEN'S INFOSEC AGENCY

About The Author

Marwyn Allen is an Information Security enthusiast and business man. Marwyn Allen, originally born and raised in Jamaica came to America in 2011 to pursue his business and education goals. Marwyn has worked in corporate America for over 10 years with brands such as Amazon and Truist in various roles such as Shipping Manager, IT Business Analyst, IT Support Engineer, Cyber Incident Management and Senior SOC Analyst.



Marwyn is also a serial entrepreneur that owns a consulting agency, Information Security firm and an events business. Marwyn along with his team has helped to build over a dozen brands using the skills of business management and expert business automation.

About The Author

Marwyn is a lover of nature, wildlife and true crime junkie. Marwyn spends most of days during the week building his various brands, spending time with his family, working out in the gym and binge-watching documentaries. **You can find a list of Marwyn's credentials and portfolio below:**

About The E-Book

This book was created with the intention of providing every day adults, small to medium size business owners and beginner Information Security students with general knowledge of threats, threat actors, scam techniques and ways to secure themselves and their businesses online.

The information given in this book is ever changing due to the nature of the information security industry. Readers are advised to do their own research and validation when implementing any information security protection and or policies.

Allen’s InFoSec agency is not responsible for any damage, harm or loss of finances, resources and or life caused due to any information displayed in this book.

What to Do If You Have Been Defrauded

No one wants to think about what to do if they are the victim of online fraud, but being familiar with the most important steps to take could help the whole incident become a lot less devastating.

State versus Federal Level

Fraud can be on a state or federal level in the US. If federal, the Department of Justice would be involved in the case. A case is federal depending on:

* The type of fraud

* The amount of money stolen

* The laws violated (federal, state or both)

* If public services were used, such as the U.S. Postal Service or Medicare

* The location of the crime; that is, within a state, or across state or national borders

Types of Fraud to Look Out For

Here are the main types of fraud to look out for:

* Telemarketing fraud, trying to sell fake goods or services

* Mail fraud

* Credit card and check fraud

* Identity theft

* Bank fraud

* Pyramid or Ponzi schemes

* Internet fraud

* Health care and insurance fraud

* Pension and trust fund fraud

* Fraud related to securities, commodities, and other investments

What to Do If You Are a Victim

This will depend in part on what kind of fraud you have fallen victim to, but the best policy is to inform the people who need to know right away so your legal protection can kick in. For example, if you're the victim of credit card theft, the sooner you report it, the less likely you are to be found liable for the fraudulent charges on the card.

In this case, you would notify the credit card company and file a police report. Start gathering paperwork as needed, such as a copy of the scamming web page, receipts, bank statements and so on.

1. File a police report

This will alert the police to the fraud and help put your legal protection into place in relation to, for example, what you might or might not be liable for if someone has stolen your credit card and is on a shopping spree.

2. Notify the bank and credit card company

If you used a debit card, you have 48 hours to report a fraudulent charge.

If you are having credit card issues, phone the issuer right away to freeze your account and report the status of the card, such as lost, stolen, or your statement as showing fraudulent charges.

3. Deal with the credit bureaus

Contact the three main credit reporting bureaus, Equifax, Experian and TransUnion to file a Fraud Victim Statement. Also ask them to issue a security freeze on your credit report so that no one will be able to try to get extended credit on the basis of your credit history and score.

4. Report Any Phishing

Go to https://www.consumer.ftc.gov/articles/0003-phishing to report any phishing emails you've received, or may have fallen prey to.

5. Deal with identity theft proactively

Go to https://www.identitytheft.gov/ Tell them what happened, and formulate an action plan for recovery.

6. Don't be embarrassed

Experts suspect that a lot of fraud is going unreported because people are embarrassed to admit they have been tricked by a phishing email and so on. But loss of money and personal data can have serious consequences. Plus, the more that is reported, the better chance there is of stopping the cybercriminals and helping save others from being defrauded.

Thank You!

You have reached the end of this eBook, we hope you enjoyed the summary of contents that we've put together for you. We are always looking to improve our content so please feel free to reach out to us with feedback on your experience.

We also have several other eBooks in our catalog that may interest you. Please review our website at allensinfosecagency.com for additional details.

https://allensinfosecagency.com/home/services/ support@allensinfosecagency.com