

# Synthetic ID Fraud: A refined version of Identity Theft - Cyber-Forensics.net urges to be vigilant

*Cyber hackers use an improved version of identity theft called synthetic id fraud to steal credit card information from potential individuals.*

SOFIA, BULGARIA, December 22, 2021 /EINPresswire.com/ -- Identity theft is an ever-evolving crime. As cyber forensic experts and individuals catch up to the latest schemes of identity theft, the con artists are again modifying their tactics. Scammers are now combining information from multiple individuals and inventing false identities, a "synthetic identity" theft technique.

“

when social security numbers are attached with synthetic identities, it is challenging to detect theft. And adverse credit reports get tied to genuine customers.”

*Timothy Benson, Chief Analyst*

Cyber-Forensics.net, a world-leading cyber forensic service for online scams, says scammers pull together several stolen social security or insurance numbers, abandoned property addresses, fake names, birth dates.

Using this information, the fraudsters apply for a credit card. At first, the credit card application might get rejected since scammers posing as genuine customers don't have any credit profiles. But this creates a record of a person that doesn't necessarily exist.

The scammer then adds that person to one or more legitimate accounts. Over time, they build a credible credit history. Once they are approved for a high line of credit, the con artists charge their credit cards to the limit, pay nothing, discard the fake identity, and disappear.

Timothy Benson, the chief analyst at Cyber-Forensics.net, explains, "when social security numbers are attached with synthetic identities, it is challenging to detect theft. And adverse credit reports get tied to genuine customers. This means that fraud alerts, credit monitoring, and credit freezes can't stop scammers. And as a result, unpaid bad debts affect the individuals' ability to take loans or credits.

Measures to avoid Synthetic Id Fraud Attacks

Minimize Exposure of personal information: Never share Social security numbers or social insurance numbers if not necessary. When a business individual asks for such valuable information, never be afraid to ask their id and position in the department they claim they are from

Protecting children's personal information: Since a minor cannot open a loan or credit card on their own, the lack of information in their credit history proves beneficial for scammers. A fraudster might use the child's Social security number in the same way, to: get a bank account, open a credit card, apply for a job, rent an apartment, etc.

Keep an eye on transactions: Monitor unknown phone calls, emails received. Be alert if something is amiss or sounds out of context.

What can Synthetic Id Fraud victims do if they have been scammed?

Regardless of the extent of the amount accrued by criminals, some agencies limit the account holder's liability to just a minimum charge. And many credit card companies often waive the cost altogether with zero liability policies.

Therefore, the account holder incurs no expenses or least expenses in most cases if the credit card is reported stolen and used in conducting unauthorized transactions.

This means that the customer can get their money back. But to do so, the victims need to take a few necessary steps and secure their credit account:

Contact Credit Card Company: Contact the company as soon as there is any suspicious activity. Credit card service companies can launch an investigation, verify the fraudulent activity, and immediately cancel all compromised activities.

Update Security Details: Change any compromised PINs, security information, or online passwords.

Get in touch with Credit Bureau: Contact any credit bureaus like Experian, Equifax, or TransUnion- to set up security alerts on credit reports.

Check Bank Statement frequently: Notify the bank immediately and check transaction activity to see foreign transactions.

How to get back money lost on Synthetic Id Theft?

In the event of identity theft or unauthorized use of personal information, the sooner an online victim acts, the better. Getting scammed into giving personal information is already the worst. However, recovery is about more than just gaining financial losses back. As recommended by cyber experts, the following steps can help individuals guard against further theft.

Fund Theft Insurance: Check homeowner's policy to see whether it includes coverage of fraud losses and reimbursements for identity theft-related expenses.

Consider consulting tax professionals: Calculating the fraud loss deduction can be complex. Seeking help from professional IRS agents can eliminate the complicated exceptions.

Consult a financial advisor: Losses caused by fraud require professional help from financial advisors. A financial advisor may help examine the current situation and guide the victims onto a

path to rebuild savings. Minimize interest expenses, or reduce any more spending. Recovering money lost to identity thefts: It is better to consult a lawyer or company specializing in fund recovery. The online fraud victims must ensure that services provided cover the fund recovery process charges. Check whether the agency is licensed and has a history of complaints. Also note, in many cases, asset recovery companies charge specific fees.

#### About Cyber-Forensics.net

Cyber-Forensics.net is committed to providing the most accurate tracing service for victims of online scams. Cyber-Forensics.net empowers and simplifies the process of tracking down the cyber-criminals and assists in recovering the funds and creating an atmosphere for a negotiated settlement. For more information, please visit <https://cyber-forensics.net/>.

Peter Thompson  
Cyber-Forensics.net  
+1 917-920-6613  
[email us here](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/558875945>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.