FAULKNER UNIVERSITY

Phillip Calvert <pcalvert@faulkner.edu>

ICJE News for You

1 message

ICJE, Inc. <jimrechel@icje.org>
Reply-To: jimrechel@icje.org
To: pcalvert@faulkner.edu

Thu, Mar 14, 2019 at 4:08 PM

February 2019

INSTITUTE FOR CRIMINAL JUSTICE EDUCATION

Watches, Warnings and Despair

To those who lost loved ones in the recent tornado, the cruel reality of grief and loss can often lead to despair after the reality of life without their loved ones hits home.

For those in the community working and interacting with the survivors, it is important to watch and provide the appropriate support and warnings if they detect any signs that the survivors need emotional support, or help in dealing with the loss.

In addition, those who lost their homes, but did not suffer the loss of a loved one, will also face trying times and emotional struggles rebuilding their homes and lives as well. While the loss of a home does not compare to the loss of a loved one, there will be emotional struggles as well.

For those on the ground helping, responding to the needs of the victims, with donations, contributions and hands on support, we thank you!

For those we cannot directly help, we offer our thoughts and our prayers. Thoughts and prayers do matter, and do work....for both the victims and the dedicated volunteers and charities.

Photos courtesy AL.com, ALEA, and Samaritans Purse

May His strength help you through these trying times.

-ICJE Board Members

PS: *Sgt. Robert Burroughs is reportedly recovering and faces a long road back, including rebuilding a home totally destroyed by the tornado.*

ICJE, Inc.
Newsletter Editor: Jim Rechel
To Contact Me, email me at jimrechel@icje.org

ICJE Upcoming Training

Active Listening Skills to Enhance Basic Interviewing Techniques
Advanced Interview and Interrogation
Alabama Constitutional Law Update 2017
Basic Crime Scene Investigation
Basic Interviewing
Bomb Threat Response I & II
Cold Case Investigations
Crime Scene Investigation
Criminal Behavior Assessment
Crisis Intervention Training -
Cultural Diversity and Law Enforcement-
Detecting Deception -
Domestic Violence from the Crime Scene to the Courtroom
Domestic Violence Law Update 2017-
Ethical Decision -Making for Law Enforcement Officers-
Fraud & Financial Crime-
ID Theft and White Collar Crime Schemes-
Informant Development Program-
Internet Crime Investigation-
Interrogation Strategies- Birmingham
Interview and Interrogation-
Mental Health Crisis Intervention Training 2018-
Officer Safety -
Police Misconduct
Protecting Worship Centers -
Stress Management for Law Enforcement Officers-
The Crooks are Getting Smarter

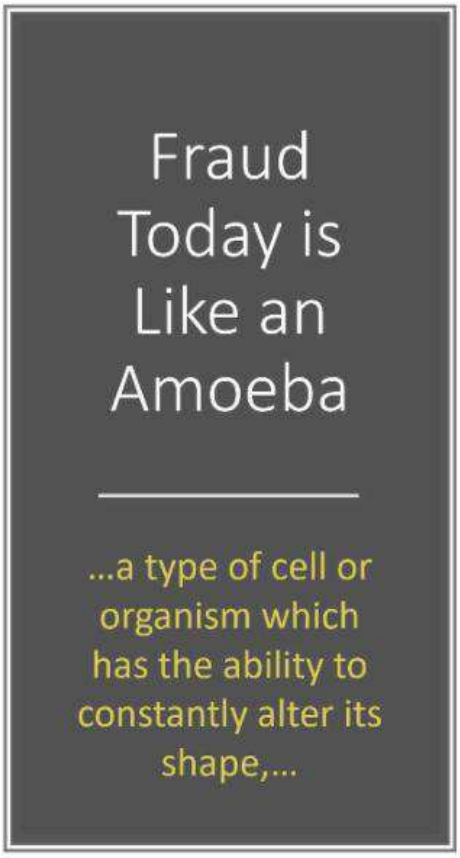
Thriving in the Fast Lane: Police Officer Survival
Using Active Listening Skills to Negotiate the Interview

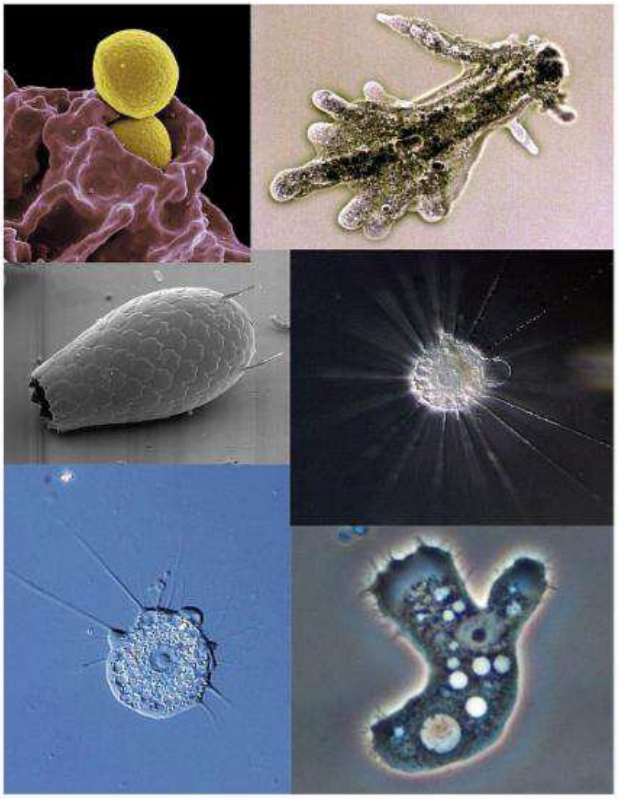
Visit the ICJE website for dates and further information.

Visit the ICJE Website

Focus on Fraud

This month's newsletter is focused on all things fraud and the trends, resources and prevention efforts available for both public and private sector personnel.





Synthetic Identity Theft Continues to Grow

To understand why "Synthetic ID Theft" and the related fraud is growing requires us to understand the manner in which private sector Credit Bureaus work.

Because the private sector does not have the same resources to validate the identity of a person representing themselves as a particular person that the public sector has, reliance upon private databases, especially credit bureau databases is critical to authenticate the identity of individuals.

In short, credit bureaus are heavily dependent upon the data provided to them by the organizations that report or make inquiries to the credit bureaus.

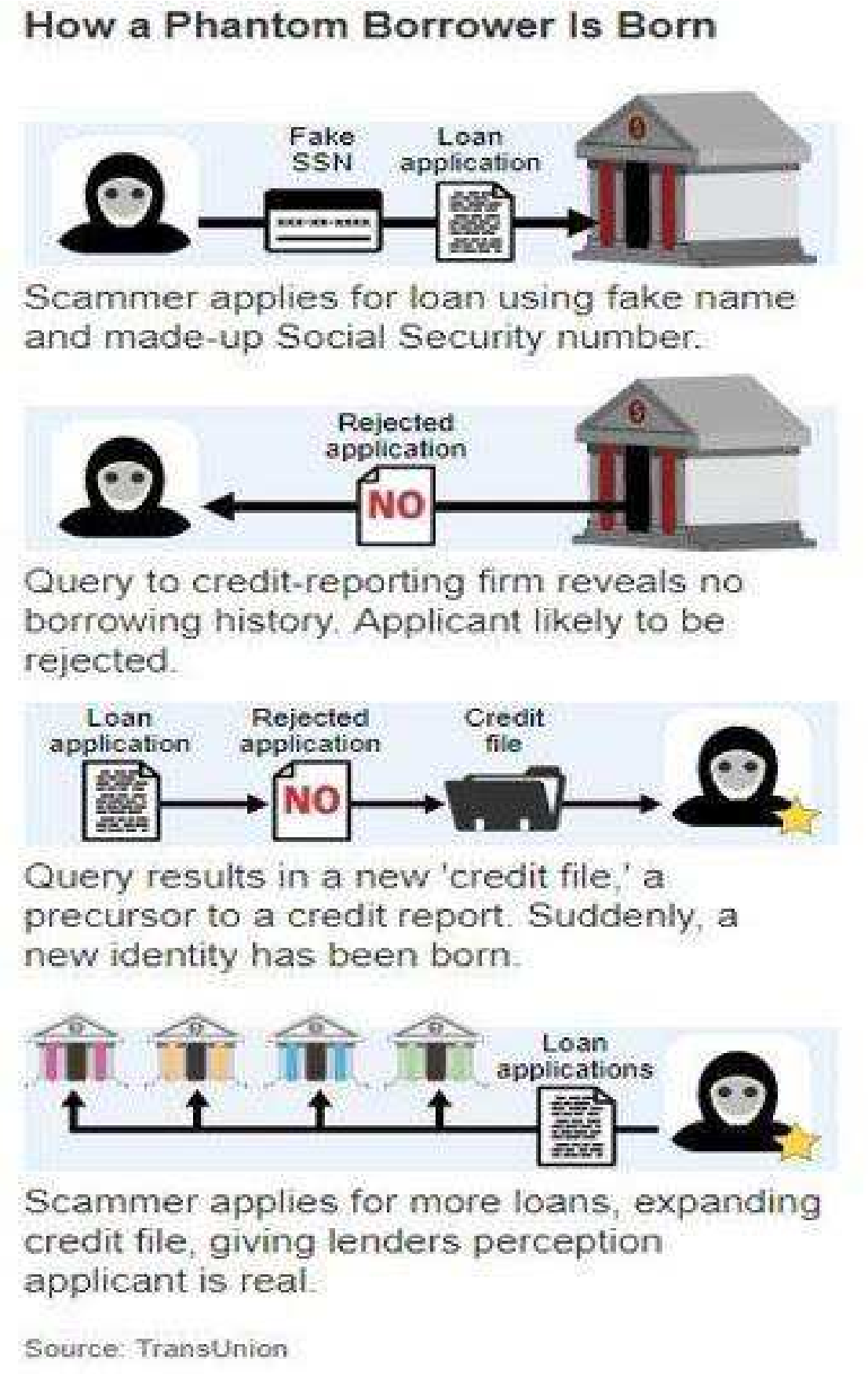
A simple example of what I mean relates to how they keep track of addresses, and therefore identities. When I moved to Alabama I never told the credit bureaus, but they eventually changed their files when I reported my address change to entities I did business with who then reported that to the credit bureaus.

When I moved to various addresses in Selma, I never notified the credit bureaus, but they eventually changed their file again. When I moved to southern Ohio they somehow caught their files up with me.

Again, because the stores, banks, and other entities I transacted with provided them the data to update their files. I never thought that I should send a change of address to the credit bureaus.

Unfortunately, the bad guys know that, and thereby fabricate identities and then have that information reported to the credit bureaus, and a hew identity is created if enough entities report the new information.

Trans Union credit bureau has a great illustration of the process, which is shown below:

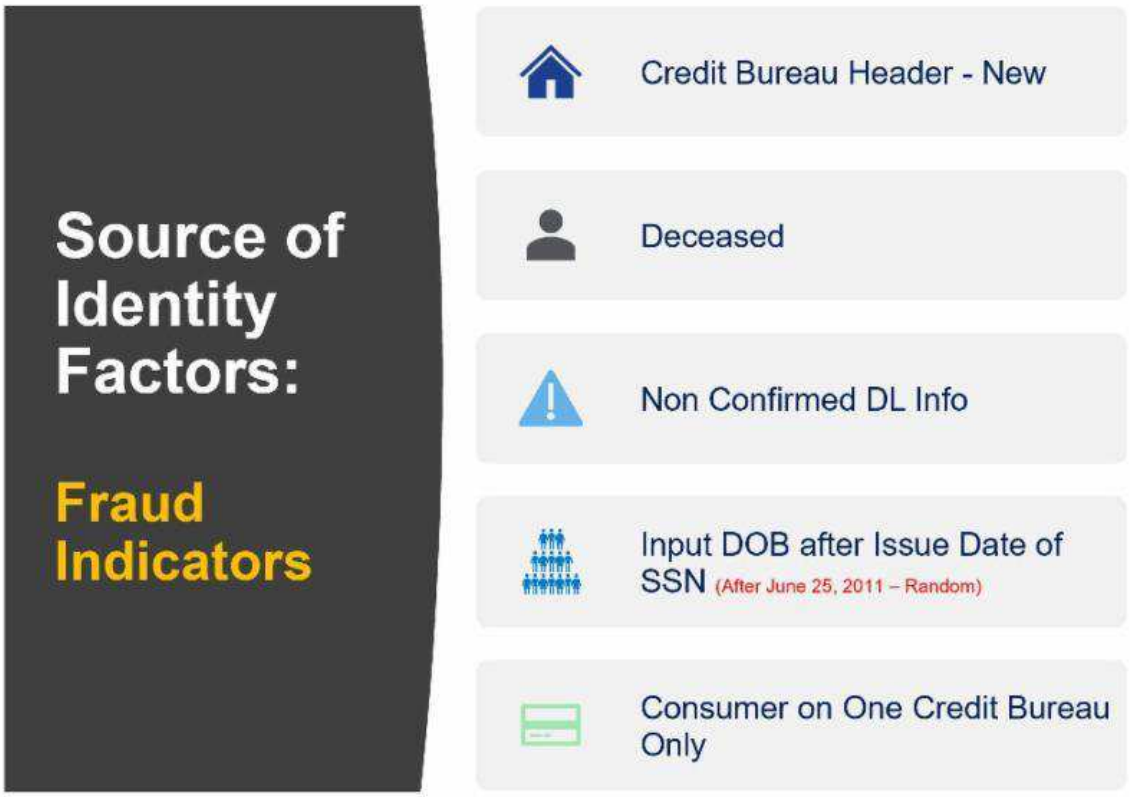


As the "credit files" are built by the fraudsters, there are some databases that can be used to compare against the identity data provided on applications which is generally not manipulated by the bad guys, and therefore is a good way to check on the legitimacy of the identifying. I put the following chart together for your reference.

In general, a review of the behavior of those fraudsters creating synthetic identities, or Digital Frankenstein's as some refer to them as, reveals that they don't do a tremendous amount of work to change other databases to match the phony information they provide to retailers and financial institutions, and to credit bureaus. This is because many of the organizations shown in the list below require either someone to physically appear to create the information in the file, or require tremendous levels of data to create the file. If the data in the files listed below match the data you are questioning, its a good chance it's not synthetic ID theft.

Red flags of potential synthetic identities include some of the following items, and extreme caution should be exercised before any actions are taken regarding any representations made to you.

1. If it appears that a new Credit Bureau Header has been created around the time you are making an inquiry to a credit bureau to verify information, especially if the DOB provided indicates that the person is not a young adult.
2. Any indication of an SSN that shows up related to a deceased individual. Fraudsters will often use the SSN of a deceased child to create a new identity. If you are conducting an investigation, and someone indicates they received pre-approved credit offers in the mail for a name they don't recognize, that can often be a red flag that someone used their address for a fraudulent application.
3. Anytime you compare your data to a state issued DL, and conflicts re present, it must be further investigated. None of the red flags stand alone, as there are many legitimate reasons that may create a mismatch of information.
4. Prior to June 25, 2011, the Social Security Administration (SSA) issued SSN's that included a ate range, so if someone input a SSN on an application or other document that included a SSN that was not issued for a specific time period of DOB's, it was a fraud indicator. However, after June 25, 2011 the SSA began randomly issuing number ranges which effectively decreased the effectiveness of this fraud indicator.
5. A significant red flag however, is if someone has a credit file created only with one credit bureau. Most legitimate individuals, have accumulated enough activity to have credit files with all three major credit bureaus.



Resources for more information and articles on Synthetic Identity Fraud:

VISA has an int4roduction website with additional links:
VISA Card Blog on Synthetic ID Fraud

In May of 2018 new legislation was passed called the Economic Growth, Regulatory Relief, and Consumer Protection Act. The Act includes a provision directing the SSA to make a mechanism available to facilitate the verification of SSNs, upon request by a certified financial institution. Currently, in order to verify an SSN, an institution must collect and submit a hard-copy wet signature on an SSA consent form, which is a significant obstacle to using current SSA services. This provision would allow a certified financial institution to obtain consent from a consumer electronically. Electronic consent will allow financial institutions to verify identities more quickly, and at scale, in connection with a credit transaction.

Further information is available from:
ID Analytics Resource Material

Lexis Nexis produced a 13 page PDF in 2017, going into much greater detail for those interested in the topic:
LexisNexis Synthetic ID Resource

Credit Bureau Connection Announces New Synthetic Identity Fraud Prevention Solution

Credit Bureau Connection

4-5 minutes

FRESNO, Calif., Jan. 21, 2019 /PRNewswire/ -- Credit Bureau Connection (CBC), the industry leader of credit reports, compliance solutions, alternative credit data, and soft pull products, announces a new Synthetic Identity Fraud prevention solution. An additional set of identity fraud detection tools created to detect and prevent this new, rapidly increasing form of fraud.

Google Warns Nest Users to Update Security Settings After Uptick of Hacked Cameras

In an email to Nest users, Google warns that everyone is a potential hacking victim.

By Sam Blum Feb 6, 2019

Many of you may have read that headline a few weeks ago, when a homeowner freaked out when someone began remotely controlling his NEST thermostat, turning it way up, then way down, messing with him the whole time, or taking over his camera and messaging.

He was convinced someone hacked into his Wi-Fi network and his NEST. It wasn't hacking, but a successful takeover of his NEST account because he used the same username and password for many of his accounts and apps. Unknown to him he was a victim of what many of us all do, using the same username and password on multiple sites.

Unfortunately, the all to common data breaches allowed the prankster to try a username and password on the NEST app, and it worked. To prevent this NEST recommends turning on a two part authorization (which I would highly recommend) to prevent this new type of fraud called "Credential Stuffing".

Informed Delivery - US Postal Service

Be on the lookout for criminals that go onto the US Postal Service and sign up for "Informed Delivery" unbeknownst to their victims.

As a result they get an email each morning, showing what mail is being delivered to the address associated with the individual.

That way the bad guy uses social engineering to order replacement credit or debit cards, fooling the financial institution employee. Instead of watching and waiting for the mail each day at the victims mailbox, the bad guy gets an email with a picture of what is being delivered to the address each day.

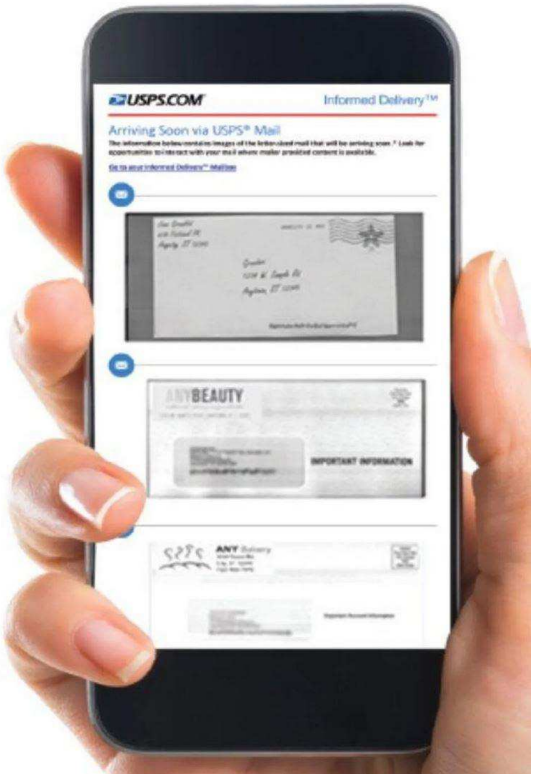
When they see the newly issued card is on its way, they know that's the day to go steal it from the mailbox. Much more efficient than the old days!

The USPS advised that on February 16, 2019, it started alerting all households by mail whenever anyone signs up to receive these scanned notifications of mail delivered to that address. The notification program, dubbed “Informed Delivery,” includes a scan of the front of each envelope destined for a specific address each day.

My thought on that is now the bad guys will sign up for the email alert, physically check for the mailed notification, and grab that before their victim knows anything is up.

The best way I can see to stop this is to either put a Credit Freeze on your credit bureau as the USPS says they don't allow Informed Delivery emails to be established for consumers with Credit Freezes, or another way to thwart the bad guys is for all the good guys to establish Informed Delivery before the bad guys set it up. Just a thought.

By the way, it's a cool service for the good guys!



Thought of the Month

There are three things in the world that deserve no mercy, hypocrisy, fraud, and tyranny.

Frederick William Robertson