FinCEN
FINANCIAL CRIMES ENFORCEMENT NETWORK

Intelligence Assesment

Intelligence Division

(U//LES) Financial Institutions Lose Tens of Millions of Dollars to Synthetic Identity Fraud

8 August 2017

(U//LES) Financial Institutions Lose Tens of Millions of Dollars to Synthetic Identity Fraud

(U//LES) Executive Summary: The ease of creating synthetic identities to acquire credit enables criminals to defraud tens of millions of dollars annually from financial institutions, according to our analysis of sensitive financial information acquired by FinCEN, open source reporting, and interviews conducted with law enforcement. Some law enforcement investigations involve tens of millions of dollars defrauded from financial institutions by criminals using synthetic identity fraud, according to law enforcement officials interviewed by FinCEN. Criminals facilitate synthetic identity fraud when they create new identities using fabricated credentials, or a combination of fake information with personally identifiable information (PII) associated with real people. Criminals then build a positive credit history and credit score for each synthetic identity to acquire credit cards, auto loans, and other lines of credit that they ultimately defraud.

- (U//LES) In 2015 and 2016, financial institutions filed 9,288 sensitive financial reports, with suspicious activity totaling $102.2 million, containing "synthetic identity" fraud in the narratives, representing a 17 percent increase in filings year to year. Financial institutions also may be reporting instances of synthetic identity fraud as *true-identity theft* or be underreporting these instances.[a]

- (U//LES) Law enforcement officials indicate gangs and other criminal organizations are adopting synthetic identity fraud and other fraud schemes to generate funds because of the ease in executing these schemes and lighter criminal sentences than those imposed for drug-trafficking offenses.

- (U//FOUO) A record number of data breaches and the widespread availability of stolen credentials help fuel the market for social security numbers (SSNs) and other information that criminals use to build synthetic identities.[1]

(U//LES) We assess synthetic identity fraud will increasingly appeal to criminals seeking easy methods to generate illicit proceeds. Our analysis indicates domestic and foreign terrorist organizations may consider the use of synthetic identity fraud as a viable technique to conceal the identities of operatives and to raise illicit proceeds to support their operations.[2] [3] [4]

[a] (U//LES) Criminals facilitate true-identity theft when they misuse the actual personally identifiable information (PII) of a real person versus fabricating an identity when facilitating a synthetic identity fraud scheme.

(U) An Easy Crime that Yields Big Rewards

(U//FOUO) Synthetic identities are relatively simple for criminals to manufacture using fabricated credentials or fake information in combination with personally identifiable information (PII) associated with actual people. For example, a criminal can misuse a social security number (SSN) belonging to a child, combined with a fictitious name and date of birth (DOB), to create a synthetic identity.[5] A synthetic identity also can consist of a random SSN combined with a real name and DOB. Some credit-repair service providers offer Credit Privacy Numbers (CPNs) to consumers seeking to build an alternative line of credit, often because their own credit rating is poor.[b] [6]

(U//FOUO) Building a positive credit history, known as *pollinating*, associated with a synthetic identity involves detailed but rudimentary processes. Techniques for establishing a good credit history and credit score tied to a synthetic identity are common, including:[c] [7]

- (U//FOUO) **Building credit over time** is a technique where criminals apply for a credit card through a major card issuer using a synthetic identity and receive a credit card with a relatively low credit limit. Once acquired, criminals use the credit card to make minimal purchases, like cell phone payments, to increase the credit score of the associated synthetic identity and apply for other cards with larger lines of credit.

- (U//FOUO) **Credit boosting,** or piggy-backing, involves a person, also called a **pollinator**, with a good credit score adding a synthetic identity, with no credit history, onto their credit card as an authorized user to jump-start the credit score of the synthetic identity.[8]

- (U//FOUO) **Using fake furnishers** helps criminals to fraudulently improve the credit scores of individuals (real and synthetic) by indicating the furnisher extended credit to them.[9] **Furnishers** are entities that provide consumers with credit, including credit card companies, mortgage lenders, automobile lenders, and department stores, that report credit data to credit bureaus.

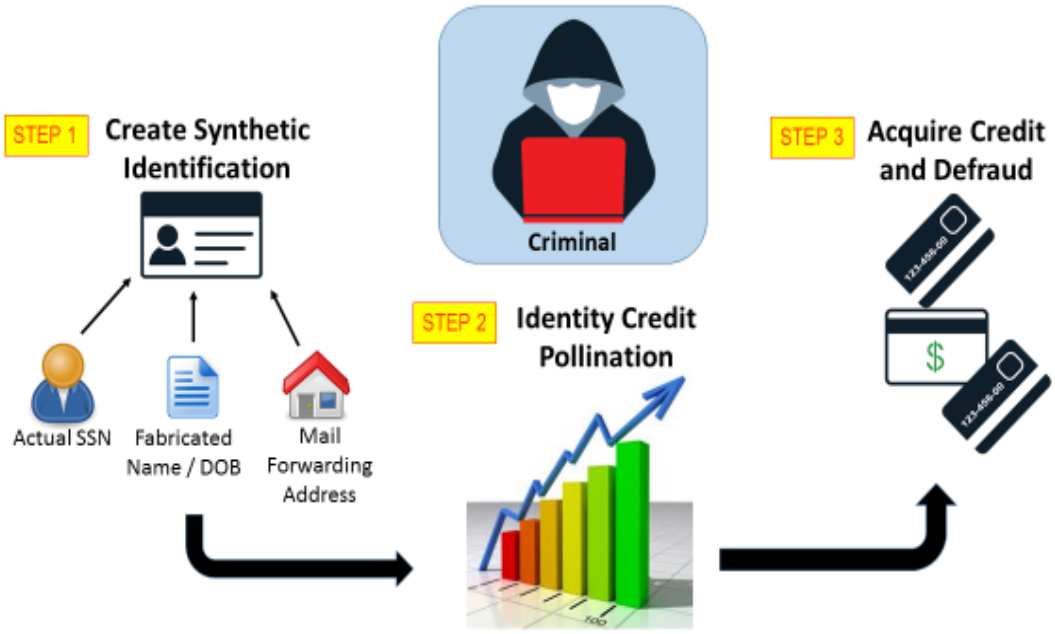
[b] (U) Also known as fraud for credit repair, this activity occurs when an individual creates a false identify using a stolen or fake SSN combined with his or her real name to build an alternate credit history. For additional information, see U.S. Government Accountability Office, *Highlights of a Forum: Combating Synthetic Identity Fraud*, July 2017, available at www.gao.gov/products/GAO-17-708SP.

[c] (U//LES) Criminals that specialize in synthetic identity fraud may create synthetic identities that remain dormant for years before executing a fraud to yield the best credit score possible and obtain multiple lines of credit, according to discussions with law enforcement.

(U//LES) Criminals use synthetic identities, with established positive credit scores, to acquire credit cards, auto loans, and other lines of credit they ultimately defraud or "bust-out."[d] Criminals can use a single synthetic identity to acquire several credit cards issued from different financial institutions. Bust-outs are usually planned for larger amounts of funds, such as a credit card with a $20,000 credit limit. Criminals withdraw funds from these lines of credit through wire transfers, cash withdrawals, or merchandise purchases that are resold or fenced for cash, according to law enforcement.

(U//FOUO) The graphic below illustrates common steps a criminal may take to facilitate synthetic identity fraud.[e]

(U//LES) Figure 1. Common Synthetic Identity Fraud Cycle



The figure above is (U//LES).

[d] (U) "Bust-out" occurs when a fraudster increases the spending limit of a credit line by paying off small purchases with the goal of obtaining larger loans. Eventually, the fraudster will "bust-out" the entire credit line, acquiring the proceeds from a large loan with no intention of paying it back. For additional information, see ID Analytics, *Exploring the Impact of SSN Randomization,* 2014, available at http://www.idanalytics.com/media/Exploring-the-Impact-of-SSN-Randomization.pdf.

[e] (U) Appendix A provides a more in-depth discussion on methodologies criminal organizations use as part of executing synthetic identity fraud schemes.

(U//LES) Criminal organizations that execute synthetic identity frauds cause large financial institution losses, according to law enforcement.[f] A criminal organization may manufacture and manage hundreds of synthetic identities at any one time, as noted in the cases below:

- (U) In 2013, law enforcement charged eighteen subjects in an international $200 million credit card fraud scheme that included criminals using synthetic identity fraud to orchestrate their schemes. This included the manufacturing of approximately 7,000 false identities to fraudulently obtain tens of thousands of credit cards.[10]

- (U) In 2016, a subject pleaded guilty to conspiracy stemming from a fraud ring that created synthetic identities to obtain credit cards. The subject and his co-conspirators created fake businesses to process the credit card transactions as part of a scheme that yielded millions of dollars in fraudulently-obtained proceeds.[11]

(U) Factors Driving Synthetic Identity Fraud

(U//LES) A record number of data breaches and the widespread availability of stolen credentials help fuel the market for SSNs and other information used to build synthetic identities.[12] The Identity Theft Resource Center (ITRC) reports that in 2016 data breaches in the United States reached an all-time high of 1,093 incidents, exposing tens of millions of records to state-sponsored hackers and cyber criminals.[13] In just four data breaches that occurred in 2015, an estimated 150 million SSNs were exposed.[g] Criminals frequently sell stolen credentials to other criminals through carding websites and darknet marketplaces to facilitate true-identity theft and build synthetic identities.[h]

[f] (U//LES) Some law enforcement officials interviewed identified potential increases in synthetic identity fraud in their Area of Responsibility (AOR) in recent years. Quantifiable data to measure the magnitude of synthetic identity fraud is limited because of the absence of individual victims reporting to law enforcement.

[g] (U) Those breaches included Mobile/Experian (15,000,000 records); U.S. Office of Personnel Management (21,500,000 records); Premera Blue Cross (11,000,000 records); and Anthem, Inc. (78,800,000 records). Refer to http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf for more information.

[h] (U//LES) Darknet marketplaces allow users to anonymously exchange value with other users for the purchase of illicit goods and services from participating vendors or sellers. Hundreds of criminals sell stolen PII through these sites. For example, located on one of the largest darknet market places, AlphaBay, are listings for the sale of CPNs with names, addresses, DOBs, and credit scores.

(U//LES) The migration to Europay, MasterCard, and Visa (EMV) chip-enabled cards in the United States likely caused criminals to increase their use of synthetic identity fraud and other fraud types, according to FinCEN analysis and law enforcement officials.[14] EMV prevents criminals from creating cloned cards where the use of stolen or compromised credit card data was essential, causing a shift in the types of frauds in which criminals now engage. Criminals are shifting to card-not-present transactions and targeting e-commerce sites to facilitate fraud, according to Javelin Strategy and Research.[i] Criminals also engage in other fraud schemes like true-identity fraud and business email compromise (BEC) schemes to fill the void left with the migration to EMV.

(U//LES) Penalties for white-collar crimes like synthetic identity fraud are typically less severe than sentences for narcotic trafficking and other street crimes, according to law enforcement officials interviewed.[j] In many instances, law enforcement officials observed narcotics traffickers switching to synthetic identity fraud schemes given the lower risk of compromise and less severe sentencing guidelines.[15] [16]

(U//LES) Synthetic Identity Fraud Reporting Increasing, But Still Underreported

(U//LES) Financial institutions are the largest victims of synthetic identity fraud and experience unique challenges in detecting and reporting this activity.[17] Financial institutions normally detect fraud affecting their financial products and services through account holder notifications and through automated alert systems.[k] Without a self-reporting victim, financial institutions face challenges in identifying and measuring the occurrence of this fraud.[18] Law enforcement officials credit the surge in synthetic identity fraud targeting financial institutions to this difficulty in detecting the activity.

[i] (U) Javelin Strategy and Research reported in a 2017 study that identity fraud affected 15.4 million consumers in 2016, a 16 percent increase from 2015. Refer to https://www.javelinstrategy.com/coverage-area/2017-identity-fraud for more information.
[j] (U//LES) FinCEN interviewed law enforcement, prosecutors, and other officials located across the country from the United States Postal Inspection Service (USPIS), Federal Bureau of Investigation (FBI), United States Secret Service (USSS), Homeland Security Investigations (HSI), Department of Justice (DOJ), Social Security Administration (SSA), Federal Trade Commission (FTC), and State and local law enforcement agencies. FinCEN also interviewed academic and industry subject matter experts in synthetic identity fraud as part of its research.
[k] (U//LES) Law enforcement officials do not typically target synthetic identity fraud because there is no victim other than a financial institution. Criminals are attracted to using synthetic identities because no individual victim exists to monitor and detect fraudulent charges on a credit card or an account, unlike schemes undertaken in true-identity theft cases.

(U//LES) Our analysis of sensitive financial information acquired by FinCEN indicates an increase in synthetic identity fraud tied to credit card fraud and auto loan fraud. In 2015 and 2016, financial institutions filed 9,288 sensitive financial reports (4,275 in 2015 and 5,013 in 2016) totaling $102.2 million, identifying the term synthetic identity in the narratives. This represents a 17 percent increase in filings from 2015 to 2016.[l]

(U//LES) Financial institutions are likely reporting instances of synthetic identity fraud as true-identity theft or underreporting synthetic identity frauds. One bank filed 87 percent of the 9,288 sensitive financial reports analyzed by FinCEN, mainly for credit card and automobile loan related frauds or fraud attempts, indicating that most banks are not recognizing or filing on this activity. Financial institutions likely classify synthetic identity fraud in a more general category of identity theft for filing purposes.[m] Underreporting also may occur when financial institutions cannot detect synthetic identity fraud (e.g., cases where a default of a credit card account is categorized as a credit or loss, as opposed to a fraud).[19]

(U//LES) Our analysis of sensitive financial information and interviews conducted with law enforcement indicates criminals likely use synthetic identity fraud to exploit financial institutions by establishing, then misusing, accounts and other lines of credit. Examples include criminals who:

- (U//LES) Use synthetic identities to open demand deposit accounts (DDAs) at depository institutions, and subsequently use the accounts to deposit counterfeit checks.
- (U//LES) Apply for unsecured personal loans through online credit lending institutions using synthetic identities.
- (U//LES) Establish accounts using synthetic identities to launder the proceeds of criminal activities. [20] [21]

(U//LES) Sensitive financial information collected by FinCEN revealed one case in which a suspected domestic terrorist organization allegedly used synthetic identity fraud to obtain and bust out credit cards.[22] Foreign terrorist organizations used false identifications to conceal their members' identities and their supporters used credit card bust-out schemes and other frauds to raise money. [23] [24] [25] We expect terrorist organizations and their supporters to increase their use of synthetic identity fraud

[l] (U) In a recent U.S. Government Accountability Office report, industry experts indicate synthetic identity fraud has grown significantly in the past five years and has resulted in losses exceeding hundreds of millions of dollars to the financial industry in 2016. For additional information, see U.S. Government Accountability Office, *Highlights of a Forum: Combating Synthetic Identity Fraud*, July 2017, available at https://www.gao.gov/products/GAO-17-708SP.

[m] (U) 16 CFR Part 603.2(a) defines identity theft as a fraud committed or attempted using the identifying information of another person without authority.

because the activity is relatively simple to execute to generate illicit proceeds and create synthetic identities to conceal the source of funds.[26] [27]

(U) **Customer Identification**: The Bank Secrecy Act (BSA) requires banks to implement a written Customer Identification Program (CIP) appropriate for its size and type of business. The CIP must (a) obtain, at a minimum, three key pieces of personal information (full name, DOB, and SSN [or passport information for non-residents]), and (b) include risk-based documentary or non-documentary procedures for verifying the identity of each customer to the extent reasonable and practical.[n] This study does not assess the extent financial institutions rely solely on credit checks to comply with CIP rules, and the warranties of the credit check agencies about the veracity and accuracy of their information are not clear.

(U//LES) Uncloaking Synthetic Identity Theft

(U//LES) FinCEN's study of synthetic identity fraud supports the need for greater collaboration among the law enforcement and regulatory communities and the financial industry to combat this growing fraud trend. FinCEN will identify and monitor sensitive financial information filed for synthetic identity fraud and report emerging trends and patterns to law enforcement and regulatory agencies. FinCEN also will share synthetic identity fraud trends and financial intelligence with foreign financial intelligence unit (FIU) partners to combat transnational criminal organizations engaged in these schemes.

(U//LES) FinCEN's will research the challenges confronting financial institutions in their ability to detect and report synthetic identity fraud. Financial institutions immediately reporting suspected synthetic identity fraud is essential for law enforcement to investigate such cases. Delays in such reporting enable criminals to broaden their schemes.

(U) Note: FinCEN encourages all law enforcement agencies that have equities in the subject(s) of this FinCEN Intelligence Assessment to de-conflict case sensitive information and network.

(U/FOUO) Please contact the FinCEN Production Management Office at FinCENProducts@fincen.gov if you have any questions pertaining to this report. Reference Report #267546 and ID/OTI/IFM for routing purposes.

[n] See 31 CFR Part 1020.22.

(U) Warning Regarding Use and Dissemination

(U) The information in this document is to be used for lead purposes only. This document contains information that is protected from unauthorized disclosure by the Bank Secrecy Act ("BSA") and other laws. Unauthorized release of information contained in this document is unlawful and may result in criminal, civil, or disciplinary sanctions under the BSA and other laws, and the loss of access to information. The information may not be released, disseminated, disclosed, or transmitted outside your organization without the prior, written approval of FinCEN.

(U//FOUO) Appendix A: Criminal Methodologies Tailored for Maximum Profit

(U//LES) Criminals use synthetic identities to facilitate sophisticated fraud schemes that often yield larger fraud losses for financial institutions than losses derived from true-identity theft schemes. Synthetic identities can yield large returns for criminals because the identities do not belong to actual people who can otherwise alert financial institutions, law enforcement, and credit bureaus when they detect fraudulent transactions. In cases of true-identity theft, a criminal must work quickly to spend funds from a stolen credit card before the issuing bank freezes the card.

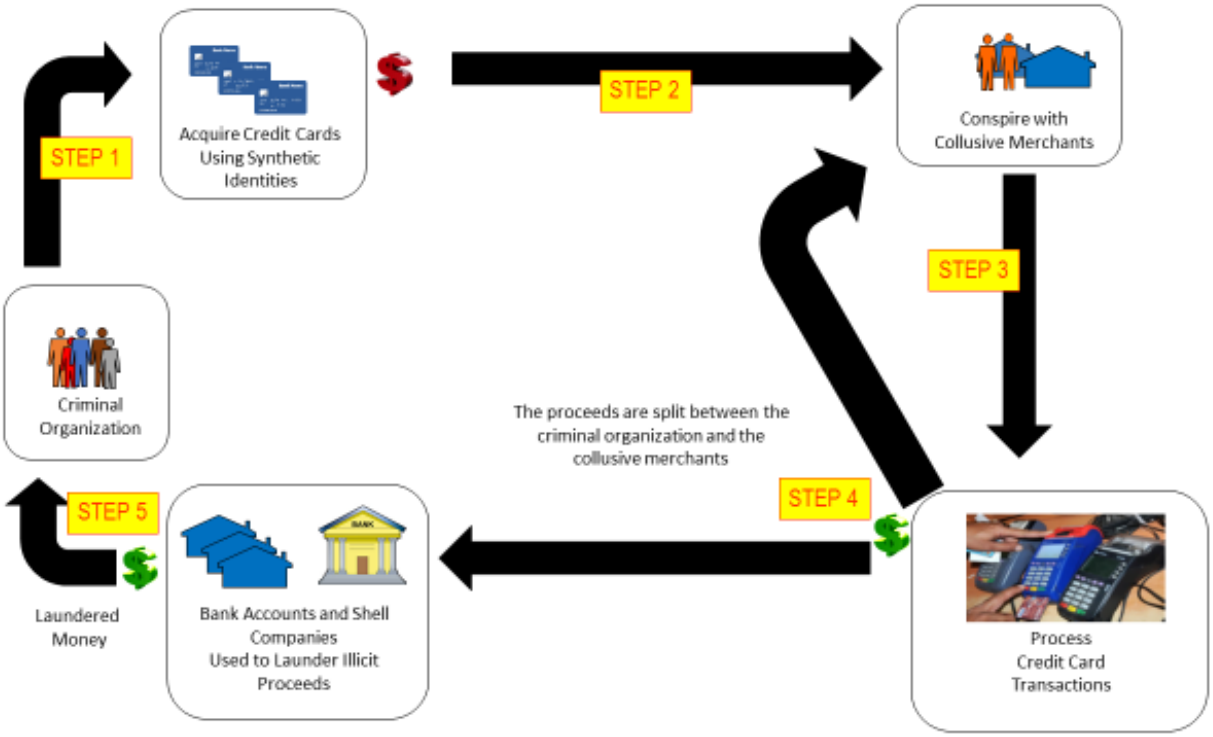
(U//LES) Advanced methodologies employed by criminal organizations to defraud financial institutions include using different types of merchants to quickly process credit card transactions obtained using synthetic identities. Some criminal organizations establish merchant accounts with financial institutions and obtain credit card point of sale equipment to process credit cards, according to multiple law enforcement sources. Law enforcement officials indicate that in many cases, criminals create shell merchants at vacant business locations where the criminals process over $100,000 in credit card transactions per month.[◦] These criminals usually establish multiple merchant accounts with different major financial institutions to maintain continuity and avoid delays in processing cards in the event of an account compromise.

(U//LES) Criminal organizations may establish actual businesses or conspire with collusive merchants to process fraudulent credit card transactions. Actual businesses include cash intensive businesses like gas stations where the processing of credit cards is common. Colluding merchants are those who conspire with criminal organizations to process credit cards acquired using synthetic identities, and in return, those merchants receive a percentage of the amount of funds processed. One law enforcement official interviewed indicated these merchants may receive as much as 30 percent commission from criminals. The colluding merchants typically pay out cash to criminals via withdrawals they make from their merchant accounts or transfer funds to another account.

◦ (U//LES) Criminals using shell businesses as merchants may incorporate these businesses using synthetic identities that provide them an additional layer of anonymity, according to law enforcement.

(U//LES The graphic below illustrates common steps a criminal may take to facilitate synthetic identity fraud.

(U//LES) Figure 2. Common Criminal Steps



The figure above is (U//LES).

[1] (U) American Banker, *Spike in Fake ID Schemes Confounds Banks' Fraud Filters*, 27 January 2015, available at https://www.americanbanker.com/news/spike-in-fake-id-schemes-confounds-banks-fraud-filters.
[2] (U) CNCnews, *Suspected Terrorist Links to Synthetic ID Fraud are Being Ignored*, 4 March 2014, available at http://www.cbc.ca/news/canada/suspected-terrorist-links-to-synthetic-id-fraud-are-being-ignored-1.2557677.
[3] (U) ID: Analytics, *Synthetic Identity Fraud Rate Increases More than 100 Percent Over Three Years*, 21 October 2014, available at http://www.idanalytics.com/blog/press-releases/synthetic-identity-fraud-rate-increases-100-percent-three-years/.
[4] (U//LES) BSA ID 31000088637156, filed on 30 June 2016.
[5] (U) Carnegie Mellon CyLab, *Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers,* 2011, available at https://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf.
[6] (U) Credit Sesame, *Your One-Way Ticket to Jail, the Credit Privacy Number*, 21 September 2016, available at https://www.creditsesame.com/blog/credit/one-way-ticket-jail-credit-privacy-number/.
[7] (U) Consumer Financial Protection Bureau (CFPB) website at https://www.consumerfinance.gov, for additional information on credit scores.
[8] (U) The Balance, *Credit Card Piggybacking and Impact to Credit Scores,* 30 August 2016, available at https://www.thebalance.com/credit-card-piggybacking-and-impact-to-credit-scores-960197.
[9] (U) United States Attorney's Office, Southern District of New York, *Participant In Multi-Million Dollar Fraudulent Credit Repair Scheme Sentenced In Manhattan Federal Court To 51 Months In Prison,* 20 March 2013, available at https://www.justice.gov/usao-sdny/pr/participant-multi-million-dollar-fraudulent-credit-repair-scheme-sentenced-manhattan.
[10] (U) Federal Bureau of Investigation, *Eighteen People Charged in International $200 Million Credit Card Fraud Scam,* 5 February 2013, available at https://archives.fbi.gov/archives/newark/press-releases/2013/eighteen-people-charged-in-international-200-million-credit-card-fraud-scam.
[11] (U) United States Attorney's Office, Central District of California, *Santa Monica Man Faces Five Years in Federal Prison after Pleading Guilty to Conspiring to Engage in Synthetic Identity Fraud,* 10 March 2016, available at https://www.justice.gov/usao-cdca/pr/santa-monica-man-faces-five-years-federal-prison-after-pleading-guilty-conspiring.
[12] (U) American Banker, *Spike in Fake ID Schemes,* op. cit.
[13] (U) Identity Theft Resource Center, *Data Breaches Report,* op. cit.
[14] (U//LES) FinCEN Executive Alert, *Steady Increase in Payment Card Fraud Reporting Shifting Criminal Tactics,* 21 December 2016.
[15] (U) The Wall Street Journal, *New York City Gangs Turn to White-Collar Crimes,* 20 February 2017, available at https://www.wsj.com/articles/new-york-city-gangs-turn-to-white-collar-crimes-1487631525.
[16] (U) ABA Journal, *More Gang Members Embrace White-Collar Crime,* 10 March 2016, available at http://www.abajournal.com/news/article/more_street_gangs_embrace_white_collar_crime.
[17] (U) United States Government Accountability Office, *Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud,* March 2017, available at https://www.gao.gov/products/GAO-17-254.
[18] (U) American Banker, *Spike in Fake ID Schemes,* op. cit.

[19] American Banker, *Identity Fraud: Back with a Vengeance, Harder to Stop,* 9 June 2016, available at https://www.americanbanker.com/news/identity-fraud-back-with-a-vengeance-harder-to-stop.
[20] (U//LES) BSA ID 31000082229690, filed on 17 March 2016.
[21] (U//LES) BSA ID 31000095446472, filed on 8 November 2016.
[22] (U//LES) BSA ID 31000094918888, filed on 28 October 2016 .
[23] (U) Testimony of John S. Pistole, Assistance Director, Counterterrorism Division, FBI, Before the House Select Committee on Homeland Security, 1 October 2003, available at https://archives.fbi.gov/archives/news/testimony/fraudulent-identification-documents-and-the-implications-for-homeland-security.
[24] (U) Department of Justice, *Four Men Charged with Providing Material Support to Al Qaeda in the Arabian Peninsula,* 5 November 2015, available at https://www.justice.gov/opa/pr/four-men-charged-providing-material-support-al-qaeda-arabian-peninsula.
[25] (U) Verafin, *A Court Case to Illustrate that Card Fraud Funded Terrorism,* 30 November 2015, available at https://verafin.com/2015/11/a-court-case-to-illustrate-that-card-fraud-funded-terrorism/.
[26] (U) CNCnews, *Suspected Terrorist Links to Synthetic ID Fraud*, op. cit.
[27] (U) ID: Analytics, *Synthetic Identity Fraud Rate Increases,* op. cit.

FinCEN Feedback Form

Please Enter the FinCEN Report Number: 267546

Product Type (SD – EA, IA, etc.): IA

Agency:

Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied Or Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied
Product's overall impact	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○
Product's timeliness	○	○	○	○	○

How will you use this product in support of your mission?

- ☐ Integrate into one of my own organization's products
- ☐ Share within my organization
- ☐ Support decision or policy-making
- ☐ Infuse/incorporate into my organization's analysis
- ☐ Share contents with partners outside of my organization
- ☐ Improve situational awareness
- ☐ Incorporate into planning and preparedness efforts
- ☐ Incorporate into training
- ☐ Use for lead investigative purposes
- ☐ Do not plan to use

How did you receive this product?

- ☐ FinCEN Email Group
- ☐ FinCEN Colleague
- ☐ FinCEN Portal
- ☐ Internal Agency Website (Please specify below)
- ☐ External/Shared Website (Please specify below)
- ☐ Other:

How could this product or its dissemination be improved? (e.g. more tactical, strategic, etc.)

Please provide your contact information to receive updates on future FinCEN training and intelligence products.

Agency:

Name:

Email Address:

Submit
Please Click Here