Grant Thornton

Session # 1

Fighting Frankenstein

The Future of Identity Crime Prevention

March 15, 2022

Speakers

James Ruotolo
Senior Manager
Fraud & Financial Crimes
james.ruotolo@us.gt.com
@jdruotolo

Taylor Larimore
Senior Manager
Fraud & Financial Crimes
taylor.larimore@us.gt.com

What We Will Cover

1 Pandemic Pressure

2 Emerging Challenges

3 Proofing and Authentication Standards

Grant Thornton

Pandemic Pressure

Current State

- Global internet usage has doubled since 2009, with more information about individuals posted online than ever before

- Fraudsters have access to more data due to massive data breaches
- Bots and the dark web provide the tools and resources for fraudsters to operate more effectively

- Structural changes have allowed fraudsters to target identity-based crimes due to:
  - Social Security Administration shifted to randomized SSNs in 2011
  - Shift to EMV (smart chip cards) sent fraudsters to digital channels in 2015

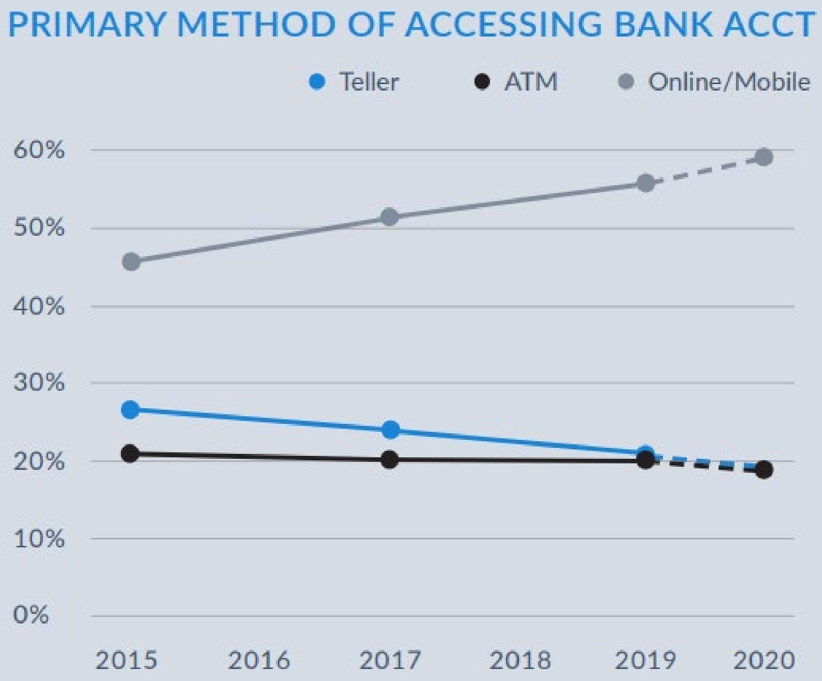
Created More Targets

Soft Targets

- PPP
- EIDL
- Unemployment Insurance

Remote Workers

- Hasty networks
- Less controls
- Less face-to-face


PRIMARY METHOD OF ACCESSING BANK ACCT

Late adopters helped move online banking ahead in 2020.

Source for 2015-2019: FDIC (2019). How America Banks: Household Use of Banking & Financial Services. 2020 estimate by FiVerity.

Speed Sacrificed Controls

- Employers set up hasty networks
- Regulators relaxed controls
- Legacy anti-fraud systems not prepared

Fraud Skyrockets

Identity Theft up
2920%

Unemployment Fraud
$400B

FRAUD
SUPER BOWL

Grant Thornton

Example

January 2022

New Jersey Man Indicted in Fraud Scheme to Steal California Unemployment Insurance Benefits

According to court documents, between October 2020 and December 2021, Jaklitsch executed a scheme to defraud the California Employment Development Department (EDD) by **filing at least 78 fraudulent unemployment insurance claims** with EDD, seeking Pandemic Unemployment Assistance and other benefits under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

During the scheme, Jaklitsch **collected personal identifying information of numerous individuals — including names, birth dates, and Social Security numbers** — and used their identities to file fraudulent unemployment insurance claims.

Polling Question #1

Have you or somebody you know been a victim of identity theft?

a. Yes
b. No

Emerging Challenges in Digital Identity Verification

ID Fraud: A large and growing problem

$1.25 Billion
Projection of US credit-card losses associated with synthetic identities for 2020

Synthetic Identity Fraud is not isolated within one industry, it is far-reaching across government and consumer industries from healthcare, banking, credit, retail, insurance, automotive, and more

1.6 Billion
The number of personal account records that have been exposed since 2005

Fraudsters using synthetic identities have learned to exploit various customer experience preferences by having a working knowledge of processes, industry reputation, and data privacy standards

Estimated that by 2023 Synthetic Identity Fraud will have resulted in
$48 Billion
in losses for lenders in the financial industry

Fraudsters can use synthetic identities to orchestrate money movement and create drop accounts from person-to-person payment tools to conventional payments

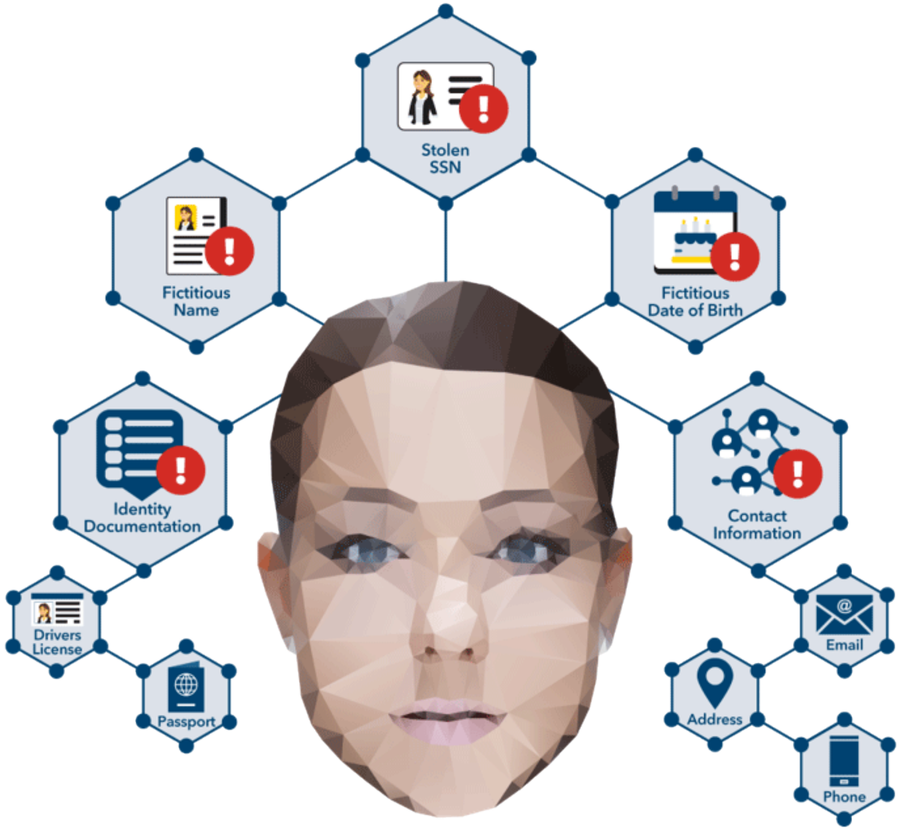
$200 Million
Amount stolen by largest synthetic identity group prosecuted using over 7,000 identities during a 10+ year timespan by 18 individuals

Though poorly understood, Synthetic Identity Fraud is the fastest growing type of Financial Crime

$1 Million
Group used identity data from over 120 children to create synthetic identities committing auto loan and insurance fraud in under 2 years

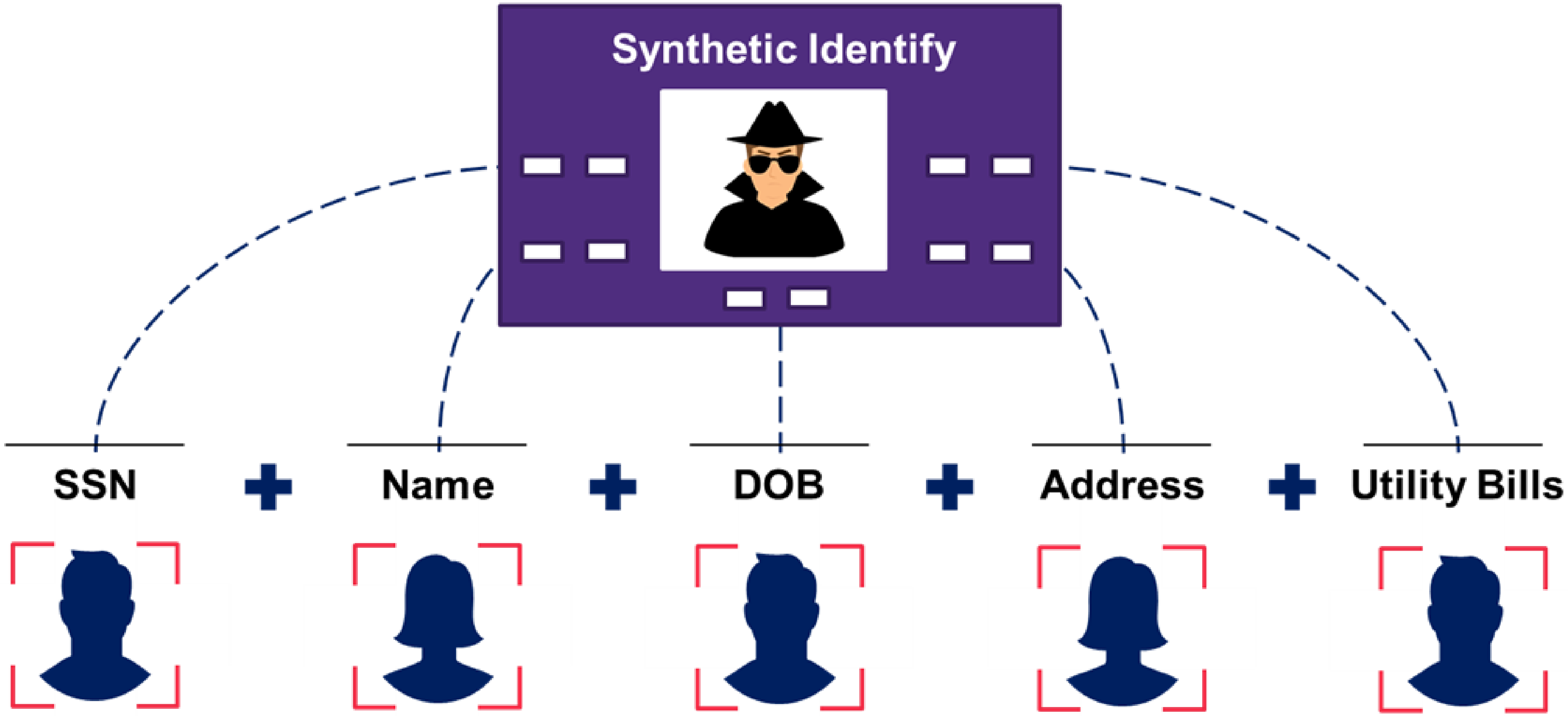
Synthetic Identity Fraud

The use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.



Source: Federal Reserve FedPayments Improvement

How it works



How it's used to commit fraud

A synthetic identity crime example

1. **Buy**
   Purchase stolen PII on the dark web.

2. **Build**
   Create synthetic identity by combining PII with bogus info.

3. **Apply**
   Apply for credit and rapidly mature a credit profile.

4. **Bust Out**
   Use all available credit and disappear.

Grant Thornton

Why it works

Scalability

Automation tools assemble millions of identities

Evasive

Extremely hard to detect

Virality

Successful profiles breed others

Common Uses

- ***Credit repair:*** Used to hide from previous negative credit history or bad debt in order to appear creditworthy.
- ***Fraud for living:*** Used to apply for employment or services (e.g., utilities, housing, bank accounts) because an individual is unwilling or unable to do so with existing primary PII elements, with no intent to default on payment.
- ***Payment default scheme:*** Used to obtain goods, cash or services with no intent to repay over a period of time.
- ***Other criminal activity:*** Used to facilitate a means to an end as part of illegal acts. *Note: These illegal acts can be conducted by individuals or groups and can include activities such as avoiding legal responsibilities, money laundering, human and/or narcotics trafficking or terrorist financing.*

Trends: Synthetic ID Fraud

Pre-Pandemic

- **Drivers**
  - SSN reliance
  - Data breaches

- **2016:** $6B (20%) of credit losses

- **2019:** "fastest growing financial crime"

Pandemic

- **2020:** $20B in losses

- **70%** of FI's say more challenging than ID theft

Example

September 2020

13 Individuals and 3 Corporations Indicted for Alleged Nation-Wide Synthetic Identity Scheme

Participants in the scheme would allegedly create synthetic identities by associating a stolen Social Security number with a different name, address and date of birth. The stolen Social Security numbers **belonged to individuals with no existing credit history or those who were unlikely to be monitoring their credit history**, such as children, recent immigrants, deceased individuals, elderly individuals, and incarcerated individuals. The defendants allegedly took steps to then make the synthetic identities appear legitimate, including **applying for phone accounts, e-mail accounts, rewards card accounts, library cards**, and other accounts with minimal verification requirements. One of the perpetrators of this scheme would also allegedly insert the synthetic identities into public databases that are used by financial institutions to verify identity information in order to further legitimize the synthetic identities.

Example

July 2021

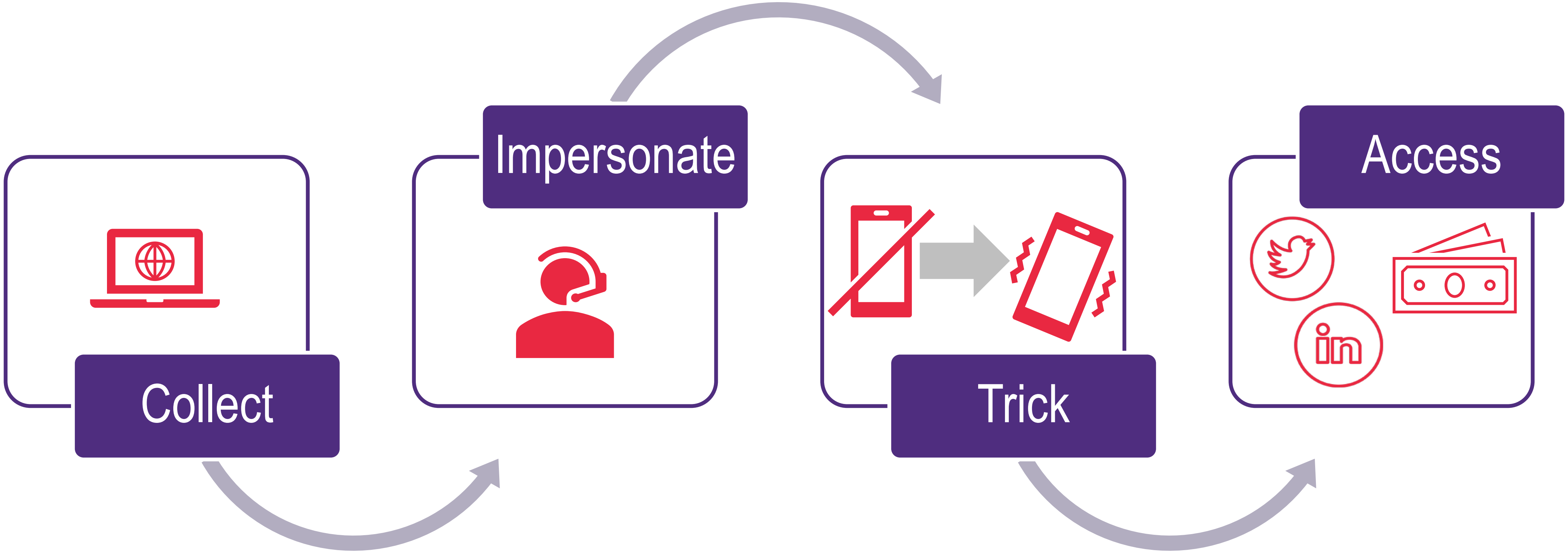
Ten Defendants in Synthetic Identity Fraud Ring Convicted of Bank Fraud, Wire Fraud, and Related Charges

The indictment charges that defendant Michael Griffin, operating from his business location in Raleigh and home in Knightdale, accepted fees from clients for alleged credit repair services. The indictment alleges that, in reality Griffin was **creating fictitious credit profiles and fraudulently altering client credit data** through the use of fictitious police reports. The indictment further charges that various defendants, many of whom were family, conspired with Griffin to defraud Synchrony Bank, a Lowe's credit card provider, by **opening credit accounts in the name of fraudulent identities, cashing out the accounts through prepaid card purchases, and then defaulting on the credit accounts**. The indictment also charges various defendants with similar frauds against other banks, including Capital One and Discover.

SIM Swapping

A malicious technique used to target mobile carriers to gain access to victim's information and accounts.

How it works



Collect

Impersonate

Trick

Access

Example

December 2021

NY Man Pleads Guilty in $20 Million SIM Swap Theft

A 24-year-old New York man who bragged about helping to steal more than $20 million worth of cryptocurrency from a technology executive has pleaded guilty to conspiracy to commit wire fraud. Nicholas Truglia was part of a group **alleged to have stolen more than $100 million from cryptocurrency investors using fraudulent "SIM swaps,"** scams in which identity thieves hijack a target's mobile phone number and use that to wrest control over the victim's online identities. Truglia is still being criminally prosecuted in Santa Clara, Calif., the home of the REACT task force, which pursues SIM-swapping cases nationwide. In November 2018, REACT investigators and New York authorities arrested Truglia on suspicion of using SIM swaps to steal approximately $1 million worth of cryptocurrencies from Robert Ross, a San Francisco father of two who later went on to found the victim advocacy website stopsimcrime.org.

Trends: SIM Swapping

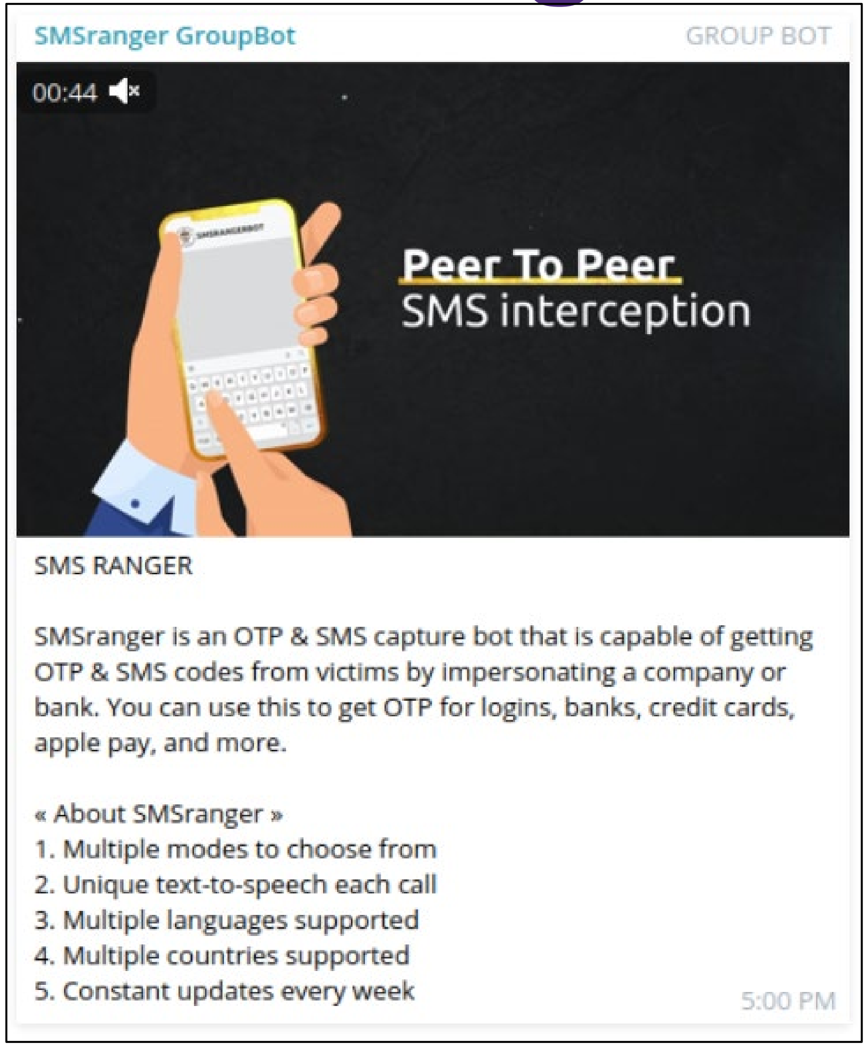
Pre-Pandemic

- An **epidemic** by 2018
- **Drivers**
  - Social Media
  - Mobile Phones
  - Cryptocurrency

Pandemic

- Vulnerable remote workers
- Mobile phishing up **328%**
- **$68M** in losses in 2021
- Rise of bots!

Phishing Bots



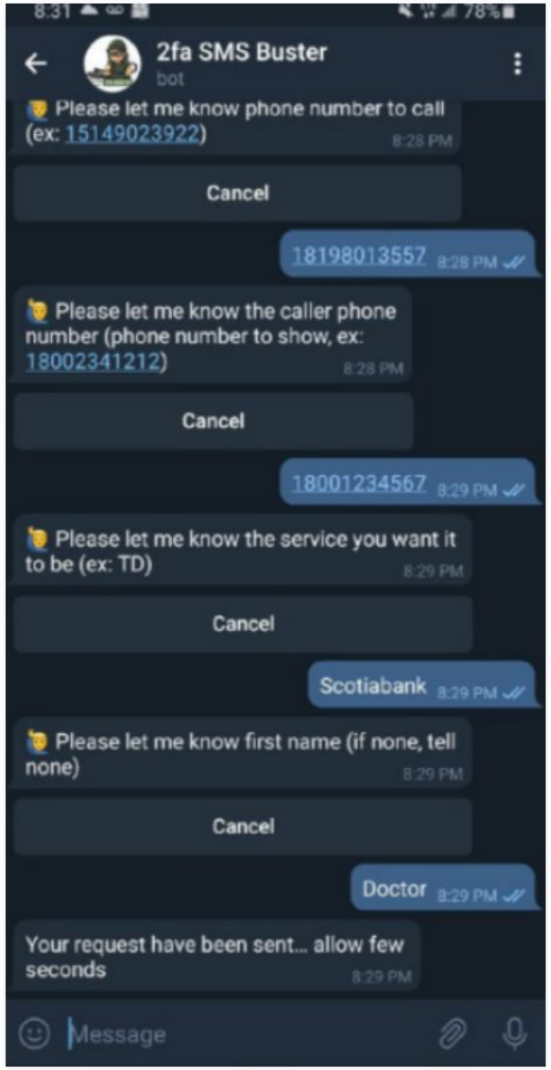
SMSranger GroupBot GROUP BOT

SMS RANGER

SMSranger is an OTP & SMS capture bot that is capable of getting OTP & SMS codes from victims by impersonating a company or bank. You can use this to get OTP for logins, banks, credit cards, apple pay, and more.

« About SMSranger »
1. Multiple modes to choose from
2. Unique text-to-speech each call
3. Multiple languages supported
4. Multiple countries supported
5. Constant updates every week

5:00 PM



2fa SMS Buster
bot

Please let me know phone number to call (ex: 15149023922) 8:28 PM

Cancel

18198013557 8:28 PM

Please let me know the caller phone number (phone number to show, ex: 18002341212) 8:28 PM

Cancel

18001234567 8:29 PM

Please let me know the service you want it to be (ex: TD) 8:29 PM

Cancel

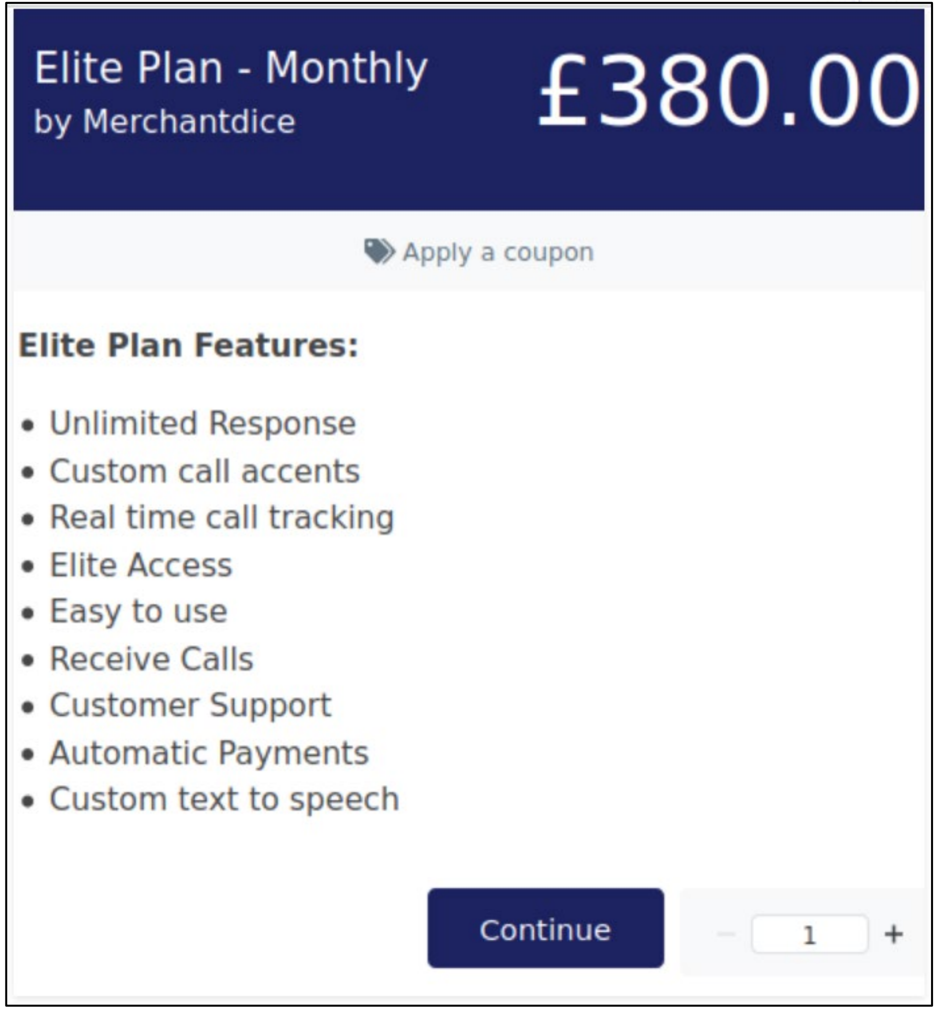
Scotiabank 8:29 PM

Please let me know first name (if none, tell none) 8:29 PM

Cancel

Doctor 8:29 PM

Your request have been sent... allow few seconds 8:29 PM



Elite Plan - Monthly
by Merchantdice

£380.00

Apply a coupon

Elite Plan Features:

- Unlimited Response
- Custom call accents
- Real time call tracking
- Elite Access
- Easy to use
- Receive Calls
- Customer Support
- Automatic Payments
- Custom text to speech

Polling Question #2

Does your organization use an identity proofing and authentication tool to help prevent and detect fraud?

a. Yes
b. No
c. Unsure

Proofing and Authentication Standards

NIST/NIST 8500 – National Institute of Standards and Technology

- NIST is a non-regulatory federal agency that sits within the US Department of Commerce
- **NIST 8500** is the standard for controls related to the development of secure and resilient federal information systems
- These controls are the guidelines used by information systems to maintain **security, confidentiality, integrity, and availability**
- Controls are divided into three risk levels known as **Identity Assurance Levels (IAL) 1, 2 and 3**. Levels are determined based on the sensitivity levels of information being accessed

NIST 8500 Details of IAL

! IAL 1

Low Risk

- Email/Password
- No identity proofing

! IAL 2

Medium Risk

- Biometric
- User must submit evidence for identity proofing, remote permitted
- Recent privacy, equity concerns related to photo storage, and 1:many

! IAL 3

High Risk

- In person
- Security Clearance types of requests/PIV request
- Physical presence is required for in person or supervised remote proofing.

Grant Thornton

NIST 8500 Details of Authentication Assurance Level (AAL)

! AAL 1

Low Risk

- Single or Multi Factor Authentication (MFA)
- No restrictions on authenticators

! AAL 2

Medium Risk

- MFA required which combines forms of authenticators
- For example, Password and an SMS code

! AAL 3

High Risk

- MFA with strict limits on the types of authenticators
- Two of the three authenticator categories
- Something you Know; Something you Have; Something you Are

Any final questions?

Q & A

Grant Thornton

The Dark Side

How Fraudsters Use The Dark Web Against The Government

What We Will Cover

1. Deep and Dark Web Overview
2. Deep and Dark Web Fraudster Profiles
3. Insight Into The Next Normal
4. Proactive Solutions
5. Reactive Solutions

Grant Thornton

Deep and Dark Web Overview

The Dark Web

FRAUD

PREVENT / DETECT / INVESTIGATE | © Grant Thornton

- Data is the most valuable commodity in modern commercial economies. Nefarious actors sell, trade, and weaponize data on a massive scale to gain access to accounts, create fictitious identities, and commit large-scale fraud.

- Today **there is a booming dark web underground market online, where criminals buy and sell identities, handbooks for how to commit fraud, forged documents and more with anonymity**. New, highly sophisticated cyber fraud schemes use techniques like phishing, spoofing, and notoriously effective malware that can “brute force” into vulnerable IT systems.

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY

5,982,772

Records

EVERY HOUR

249,282

Records

EVERY MINUTE

4,155

Records

EVERY SECOND

69

Records

It's a Buyer's Market

“The Onion Router,” (Tor), is the most popular and prolific browser for accessing the dark web.

Marketplace

$0-$100	$200-$350	$500-$1,000	$5,000-$500,000
Credit cards with T2 Freshly hacked emails DDOS attacks Hacked websites	Bomb threat as a service Biological material	Malware Access to government networks	Hits Money laundering 0-days

Finding a Target

10%

of Americans are victims of identity theft

20%

of those people are repeat victims

$1000-$1500

Price of full identity kit

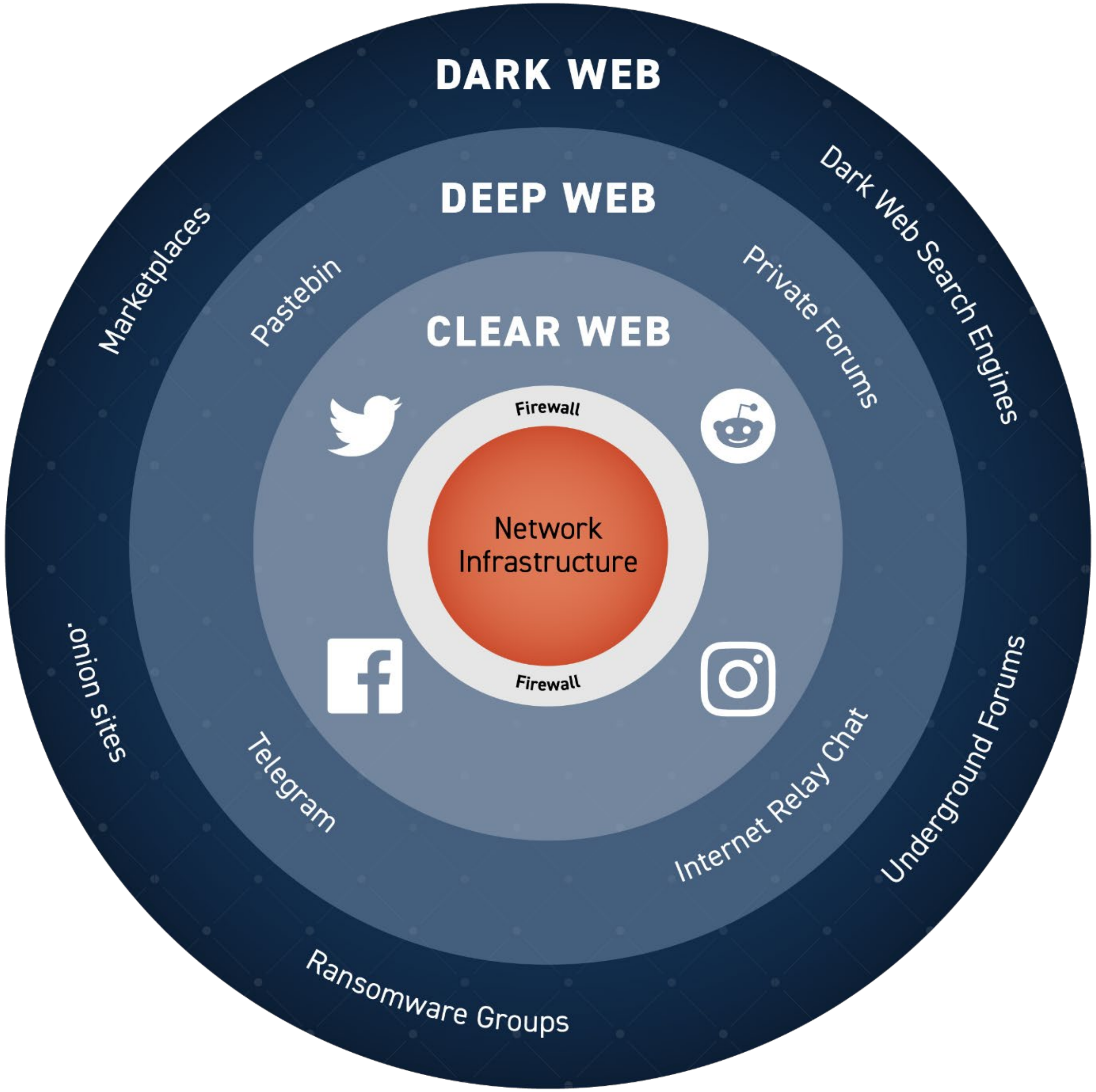
Some techniques for compiling identity kits:

- Searching credentials from previously breached databases
- Profiling high net worth individuals with open source tools
- Hacking cell phones, computers or tablets
- Creating credit monitoring reports on behalf of a victim

Total Cost: $1500

Grant Thornton

The Deep and Dark Web



How is This Used to Commit Fraud?

A synthetic identity crime example

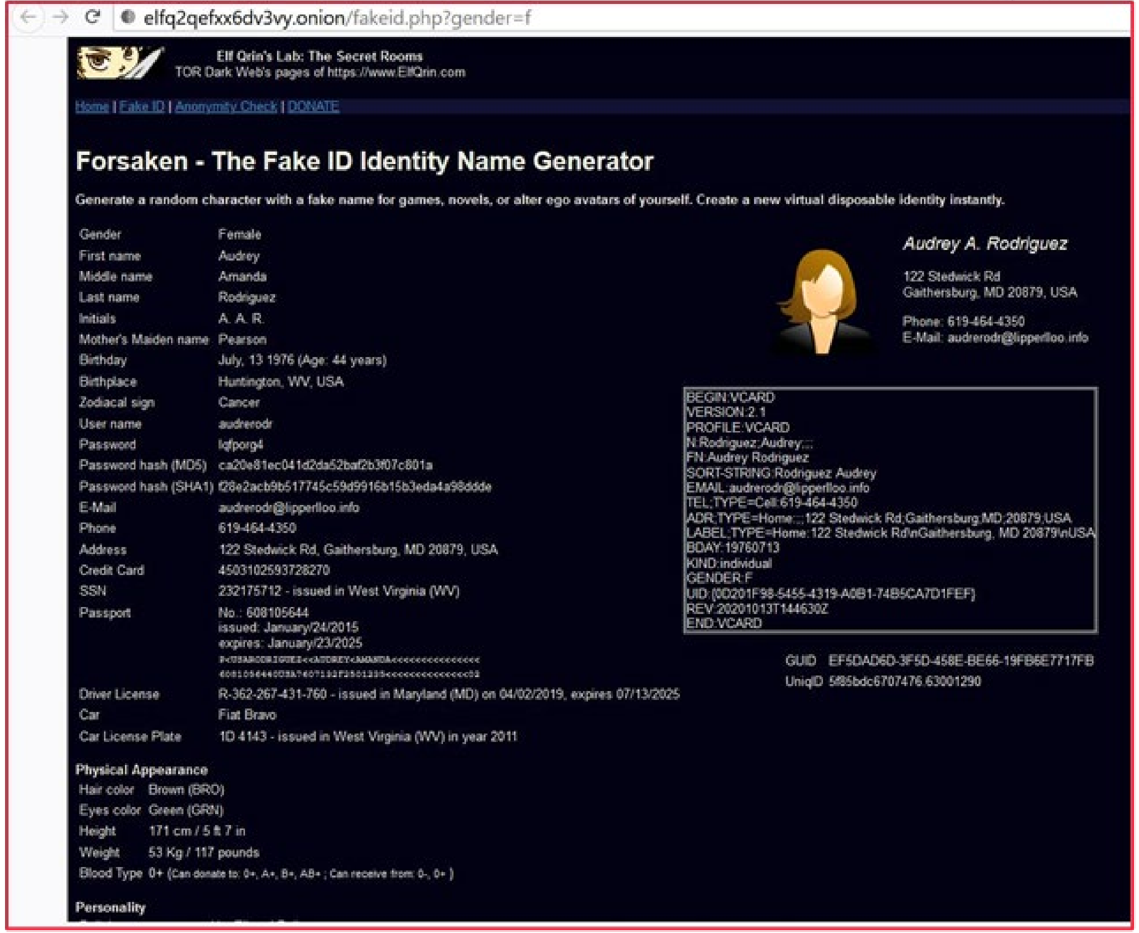
1 **Buy**
Purchase stolen PII, fabricated documents, and instructional tutorials on the dark web.

2 **Build**
Create synthetic identity by combining PII with bogus info.

3 **Apply**
Apply for government benefits with purchased PII and instructional tutorials.

Dark Web ID Generators

- As more and more interactions take place online and data breaches flood the dark web with stolen personal information, identity theft and account takeovers have become an increasingly common nightmare for consumers and a costly challenge for organizations – particularly in the case of synthetic identity fraud, one of the fastest-growing types of financial crime in the United States.
- Synthetic identity fraud is one of the fastest-growing types of financial crime in the US. Threat actors can generate PII and use this data for imitating identity and could thus be used to perpetuate fraud. The generated PII can be paired with a real valid SSN to generate a "new" synthetic identity.



elfq2qefxx6dv3vy.onion/fakeid.php?gender=f

Elf Qrin's Lab: The Secret Rooms
TOR Dark Web's pages of https://www.ElfQrin.com

Home | Fake ID | Anonymity Check | DONATE

Forsaken - The Fake ID Identity Name Generator

Generate a random character with a fake name for games, novels, or alter ego avatars of yourself. Create a new virtual disposable identity instantly.

Gender	Female
First name	Audrey
Middle name	Amanda
Last name	Rodriguez
Initials	A. A. R.
Mother's Maiden name	Pearson
Birthday	July, 13 1976 (Age: 44 years)
Birthplace	Huntington, WV, USA
Zodiacal sign	Cancer
User name	audrerodr
Password	lqfporg4
Password hash (MD5)	ca20e81ec041d2da52baf2b3f07c801a
Password hash (SHA1)	f28e2acb9b517745c59d9916b15b3eda4a98ddde
E-Mail	audrerodr@lipperlloo.info
Phone	619-464-4350
Address	122 Stedwick Rd, Gaithersburg, MD 20879, USA
Credit Card	4503102593728270
SSN	232175712 - issued in West Virginia (WV)
Passport	No.: 608105644 issued: January/24/2015 expires: January/23/2025 [illegible] [illegible]
Driver License	R-362-267-431-760 - issued in Maryland (MD) on 04/02/2019, expires 07/13/2025
Car	Fiat Bravo
Car License Plate	1D 4143 - issued in West Virginia (WV) in year 2011

Audrey A. Rodriguez

122 Stedwick Rd
Gaithersburg, MD 20879, USA

Phone: 619-464-4350
E-Mail: audrerodr@lipperlloo.info

```
BEGIN:VCARD
VERSION:2.1
PROFILE:VCARD
N:Rodriguez;Audrey;;;
FN:Audrey Rodriguez
SORT-STRING:Rodriguez Audrey
EMAIL:audrerodr@lipperlloo.info
TEL;TYPE=Cell:619-464-4350
ADR;TYPE=Home:;;122 Stedwick Rd;Gaithersburg;MD;20879;USA
LABEL;TYPE=Home:122 Stedwick Rd\nGaithersburg, MD 20879\nUSA
BDAY:19760713
KIND:individual
GENDER:F
UID:{0D201F98-5455-4319-A0B1-74B5CA7D1FEF}
REV:20201013T144630Z
END:VCARD
```

GUID	EF5DAD6D-3F5D-458E-BE66-19FB6E7717FB
UniqID	5f85bdc6707476.63001290

Physical Appearance

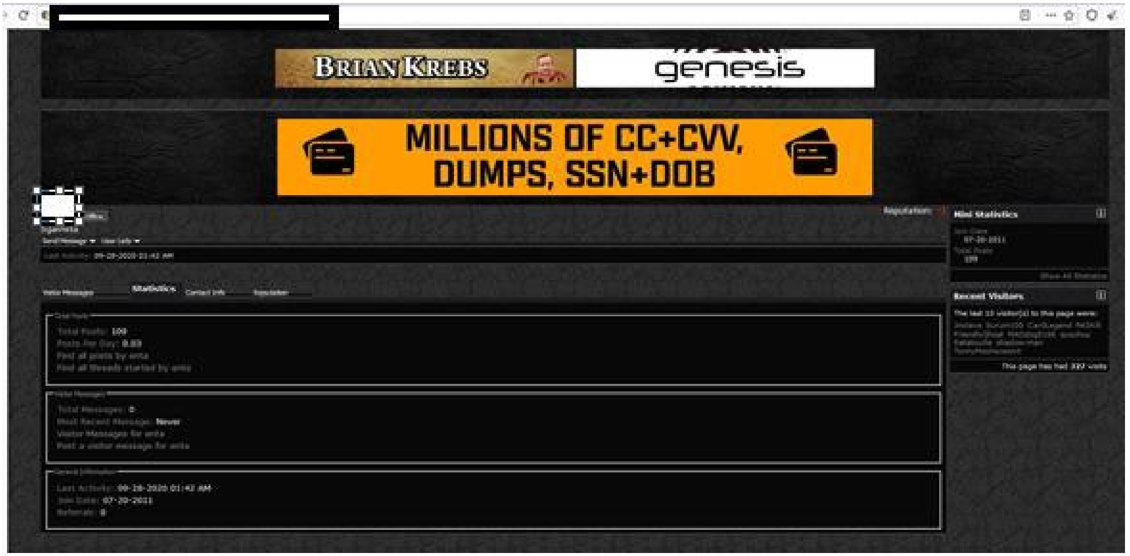
Hair color	Brown (BRO)
Eyes color	Green (GRN)
Height	171 cm / 5 ft 7 in
Weight	53 Kg / 117 pounds
Blood Type	0+ (Can donate to: 0+, A+, B+, AB+ ; Can receive from: 0-, 0+)

Personality

Dark Web Products

Counterfeit Identity Documents

The sale of personally identifiable information (PII), often obtained through a prior data breach, can be used by threat actors for a variety of fraud schemes, such as the submission of an application for unemployment benefits in the name of the unsuspecting victim.



[redacted]

BRIAN KREBS genesis

MILLIONS OF CC+CVV, DUMPS, SSN+DOB

Send Message ▾ User Lists ▾

Last Activity: 09-28-2020 01:42 AM

Visitor Messages | Statistics | Contact Info | Reputation

Total Posts: 109
Posts Per Day: 0.03
Find all posts by anta
Find all threads started by anta

Total Messages: 0
Most Recent Message: Never
Visitor Messages for anta
Post a visitor message for anta

General Information

Last Activity: 09-28-2020 01:42 AM
Join Date: 07-20-2011
Referrals: 0

Mini Statistics

Join Date 07-20-2011
Total Posts 109

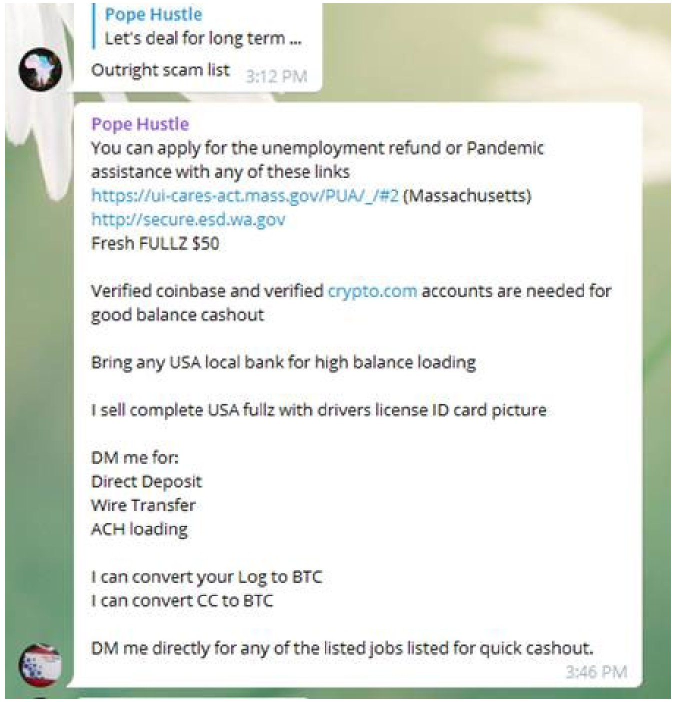
Recent Visitors

The last 10 visitor(s) to this page were: [illegible]

This page has had 392 visits

DIY Fraud Guides

Fraud guides are increasingly for sale on the Dark Web—these are instruction manuals designed to teach criminal how to ply their trade. “Fullz” includes full personal details and can be used for applying for unemployment refunds as part of the pandemic assistance.



Pope Hustle
Let's deal for long term ...

Outright scam list 3:12 PM

Pope Hustle
You can apply for the unemployment refund or Pandemic assistance with any of these links
https://ui-cares-act.mass.gov/PUA/_/#2 (Massachusetts)
http://secure.esd.wa.gov
Fresh FULLZ $50

Verified coinbase and verified crypto.com accounts are needed for good balance cashout

Bring any USA local bank for high balance loading

I sell complete USA fullz with drivers license ID card picture

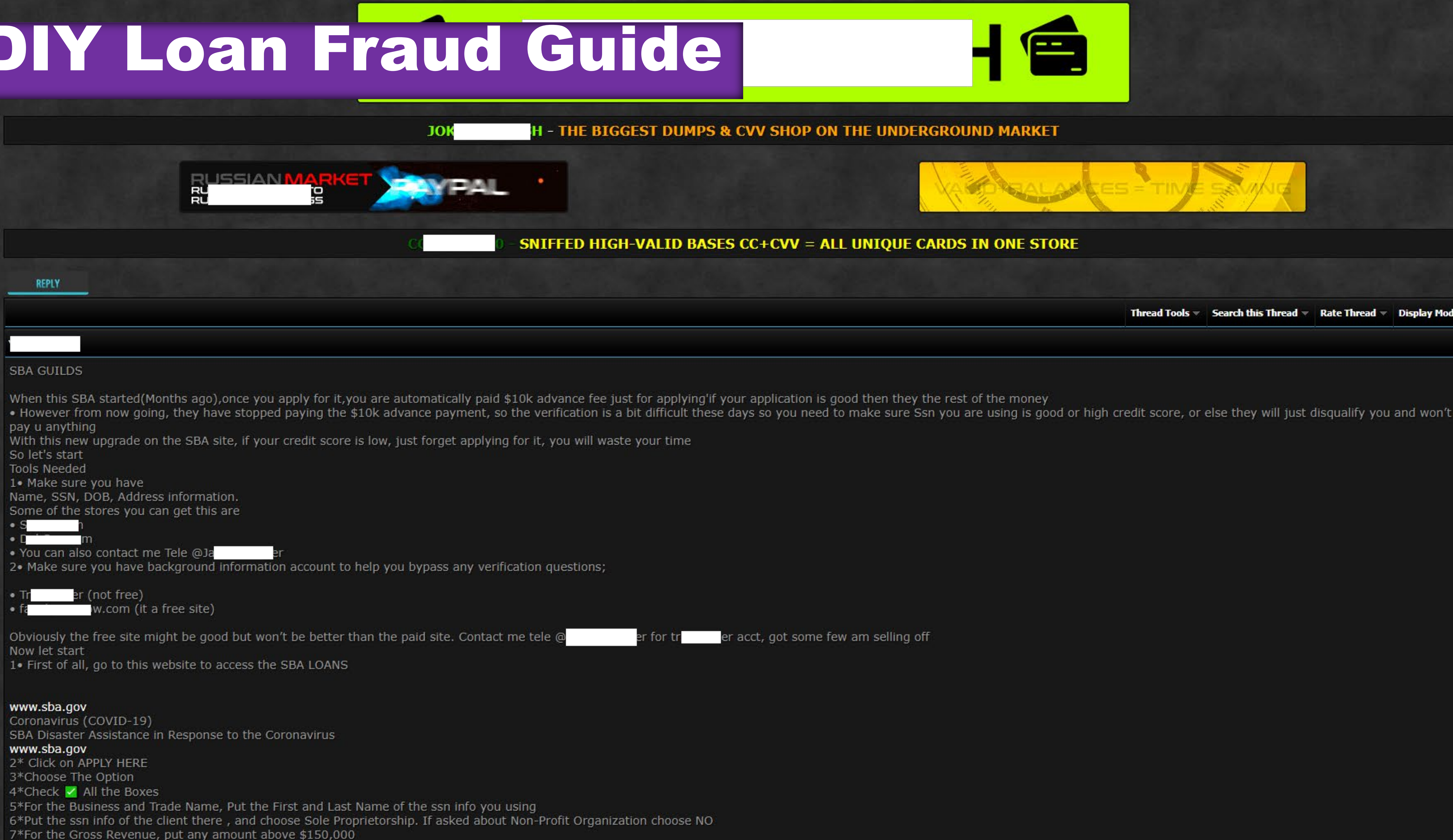
DM me for:
Direct Deposit
Wire Transfer
ACH loading

I can convert your Log to BTC
I can convert CC to BTC

DM me directly for any of the listed jobs listed for quick cashout.
3:46 PM

Grant Thornton

DIY Loan Fraud Guide



[redacted]

SBA GUILDS

When this SBA started(Months ago),once you apply for it,you are automatically paid $10k advance fee just for applying'if your application is good then they the rest of the money
• However from now going, they have stopped paying the $10k advance payment, so the verification is a bit difficult these days so you need to make sure Ssn you are using is good or high credit score, or else they will just disqualify you and won't pay u anything
With this new upgrade on the SBA site, if your credit score is low, just forget applying for it, you will waste your time
So let's start
Tools Needed
1• Make sure you have
Name, SSN, DOB, Address information.
Some of the stores you can get this are
• S[redacted]h
• D[redacted]m
• You can also contact me Tele @Ja[redacted]er
2• Make sure you have background information account to help you bypass any verification questions;

• Tr[redacted]er (not free)
• fa[redacted]w.com (it a free site)

Obviously the free site might be good but won't be better than the paid site. Contact me tele @[redacted]er for tr[redacted]er acct, got some few am selling off
Now let start
1• First of all, go to this website to access the SBA LOANS

www.sba.gov
Coronavirus (COVID-19)
SBA Disaster Assistance in Response to the Coronavirus
www.sba.gov
2* Click on APPLY HERE
3*Choose The Option
4*Check ✅ All the Boxes
5*For the Business and Trade Name, Put the First and Last Name of the ssn info you using
6*Put the ssn info of the client there , and choose Sole Proprietorship. If asked about Non-Profit Organization choose NO
7*For the Gross Revenue, put any amount above $150,000

Pandemic Fraud Triangle

Opportunity

- Access to systems and data necessary to perpetrate fraud
- Ineffective controls for a remote work force
- Reduced focus on segregation of duties

Pressure

- New employees or current employee’s spouses may have been unemployed recently
- Funding sources may have decreased, making it more difficult to obtain funding required to hit employee targets

Rationalization

- Justification that the money is only being borrowed or will be paid back when situation improves
- May feel entitled to more compensation after a year without raises or bonuses

Emerging Dark Web Pandemic Fraud Threats

Cyber Fraud as a Service

Identity Theft and Account Takeover

Organized Transnational Rings

Unemployment Insurance Fraud

Synthetic fraud and Deepfakes

Unemployment Insurance Fraud

FRAUD

Pandemic relief programs released money out the door in a swift fashion with little rigor in controls. The pandemic has been a live case study that has taught practitioners identity-based crimes are an easy common method for criminals to gain and more rigor is needed to balance the release of relief.

Up to 50% of all pandemic unemployment insurance benefits may have been paid improperly. $80 billion and counting in pandemic unemployment fraud. A significant portion of these applicants were crafted with information and tutorials bought off the dark web. Since states did not have rigorous systems in place fraudsters had an easy path.

Unemployment Benefits

Application Form

Personal Information

Surname

Given Name

Middle name

Mailing Address

City

State

Postcode

Home Address

City

State

Postcode

Occupation

Duration (yrs)

Employer Telephone

Employer Contact

Employer

Personal Information applicant 2 □ Mr □ Mrs □ Miss □ Ms

Polling Question #3

Does your organization use clear, deep, and dark web monitoring to help prevent and detect fraud?

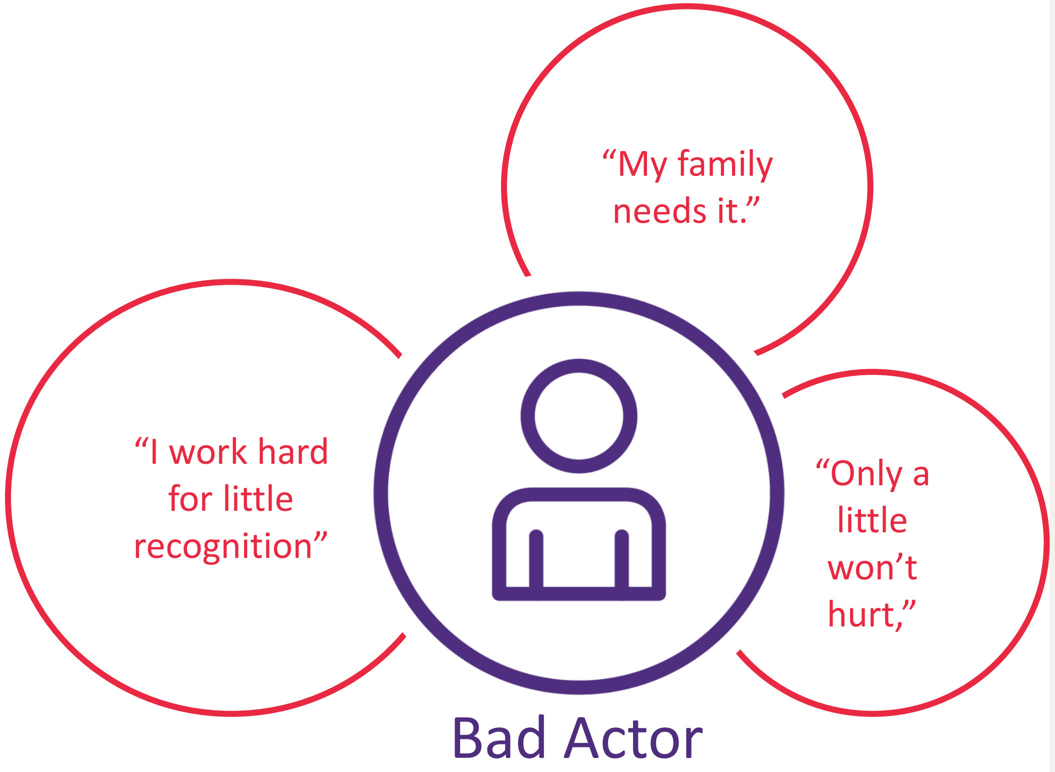
a. Yes
b. No
c. Unsure

Grant Thornton

Fraudster Profiles

Fraudster Profiles

A look at the people who
commit fraud via the dark web.


"My family needs it."
"I work hard for little recognition"
"Only a little won't hurt,"
Bad Actor

70% of Synthetic profiles have exemplary customer payment patterns making them hard to detect.

17% of internal fraudsters have control issues and are unwilling to share their duties.

Fraudsters **do not have to have** technical knowledge to commit modern schemes.

25% of internal fraudsters have financial difficulties

Grant Thornton

The Evolution of the Modern Fraudster

FRAUD

Data is the most valuable commodity in modern commercial economies.

System Breaches

Nefarious actors sell, trade, and weaponize data on a massive scale to gain access to accounts, create fictitious identities, and commit large-scale fraud.

Credential stuffing is a type of brute-force cyber attack where a fraudster tests large numbers of compromised credentials against other log-in applications

Organized criminal organizations targeting unemployment programs. Estimated 70% of the money leaving the country.

Deep fakes are synthetic media recordings that utilize machine learning technology to create fictitious audio or video

DIY fraud “how-to” guides are available to teach a new generation of cybercriminals to defraud organizations and their customers

Grant Thornton

Proactive Approaches to Combat Fraud

The best defense is a good offense

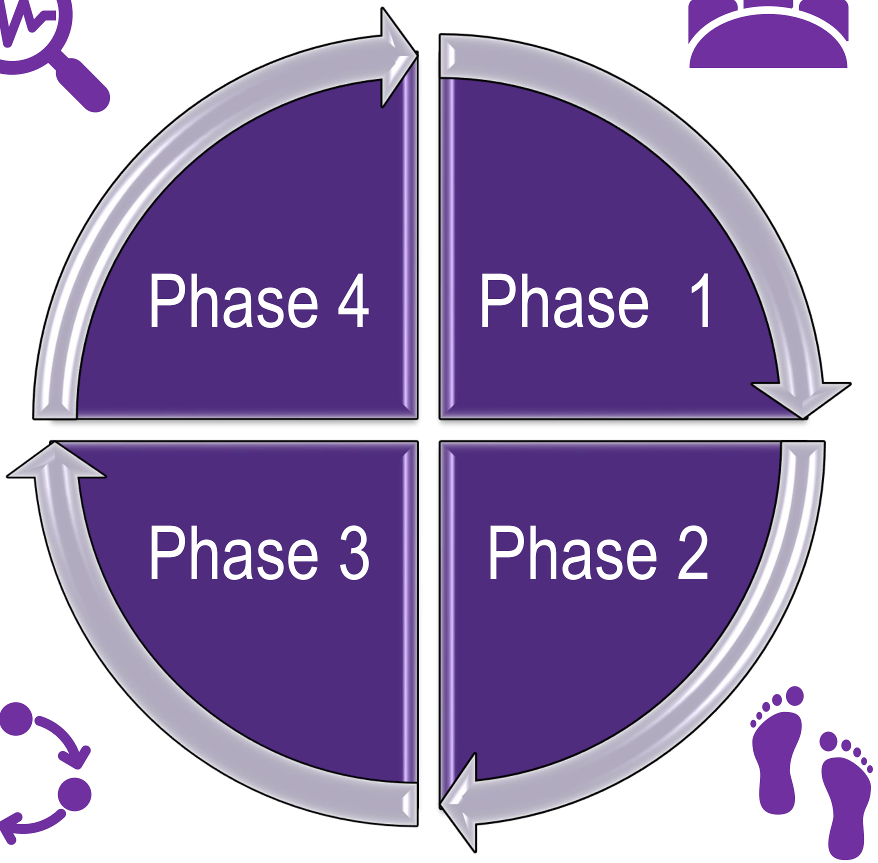
Cyber Hygiene and Intelligence

Risk Response and Monitor

As emerging threats are identified, each will require triaging and response in line with established program protocols. As part of this a tailored mitigation and action plan will be developed, documented, and implemented. Monitoring will be ongoing to oversee risk response actions and incoming threats from ongoing recon.

Ongoing Cyber Recon

Ongoing and continuous cyber recon to monitor the dark, deep and surface web, to tailored threats and human-directed intelligence that provides operational and actionable insights that can be used to develop needed risk responses in the following phase.



Establish Program Foundation

Establish and document the foundation of a cyber program, including governance, communication and reporting mechanisms and processes. This should include the identification of stakeholders to be included in risk response, and a risk response toolkit to outline a clear path from triage to risk mitigation development and deployment.

Examine Digital Footprint

Conduct an initial scan of your digital footprint to understand the current vulnerability landscape and determine priority risks and types. This will lead to the identification of gaps and vulnerabilities to be addressed prior to implementation of ongoing cyber recon, which should be integrated in line with the risk response processes developed and documented in the previous phase.

Fraud Threat Hunting

The dark web is just another part of the internet, and the internet is a tool that creates wider access and broader impact for users’ goals.

Cybercriminals operate in an underground network, but in the last few years, threat intelligence has evolved with the tools to watch them and act before they can do real damage. Today, most organizations have widely adopted threat intelligence and digital risk protection programs to inform themselves of how bad actors are targeting them.

Be Prepared

- Do we deploy state of the art of multi-factor authentication to protect against stolen credentials?
- How updated are our firewalls?
- Do our employees, clients, and third-party partners understand the precautions to thwart phishing attempts?
- Are we monitoring the deep and dark web to understand the sophistication and changing dynamics of the modern fraud scheme?
- How vulnerable are we to breached third parties?

Fraud Threat Hunting

Your **ATTACK** surface extends far beyond your network perimeter.

Challenging to see what's outside of your network

- Network security tools aren't designed for it.
- Challenging to safely get access to the places that matter.

Lack of context or relevance

- How can I VERIFY that a threat is relevant to my business?
- Lack of expertise.

Difficult decision-making

- What should I do, what is the path forward?
- What is the appropriate response?

Benefits of Fraud Threat Hunting

Proactive Risk Identification

- Gain access to where the threat actors are
- Proactive visibility into the known, unknown, and emerging threats
- Dark web, social media, open source, infrastructure

Actionable Intelligence & Insight

- Expert-curated analysis with advanced analytics
- Risk-based prioritization of threats
- Actionable recommendations on next steps to close weaknesses or gaps, in line with program governance

Enhanced Decision-Making & Planning

- Structured roles and responsibilities for handling digital threats
- Structured communication between contractors, law enforcement, states, and other program partners to combat fraud collectively

Benefits of Fraud Threat Hunting

Effective Intelligence guides focus and investment to facilitate well-informed decisions aligned with your business needs and risk appetite.

Provides the guidance necessary to make intelligence-driven actions a reality within your organization. The solution provides finished intelligence on threats specific to your organization so you can respond quickly and decisively.

- **Continuous vigilance to inform of early indications and warning of potentially fraudulent activity**
- **Improvements on how fraud threats are identified, understood, and shared throughout the organization**
- **Informed decision making for appropriate allocation of resources and proper prioritization of defense investments**
- **Insights into the efficacy of the organization's fraud prevention and detection capabilities**

Enhanced Fraud Risk Assessment

Conducting a fraud risk assessment helps an organization understand vulnerabilities and likely fraud schemes - allows for a holistic and detailed look at the internal and external fraud risks across the organization to prioritize proactive action.

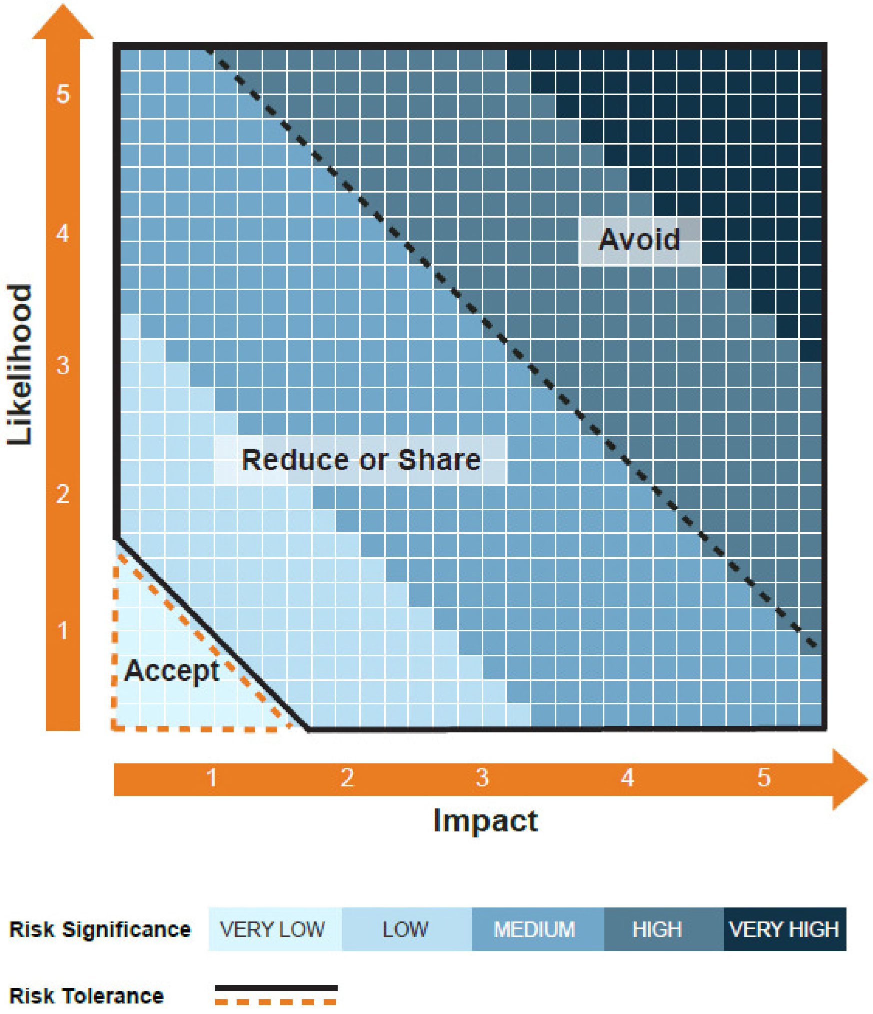
Utilize all available sources of data and tools – Advanced analytics, emerging trends, due diligence, control activities, monitoring, fraud threat hunting, and other organizational intelligence are all factors and outcomes that influence a fraud risk assessment.

The deep and dark web is an ally – The deep and dark web is a pool of data to be tapped into. Enhancing fraud risk assessments with deep and dark web intel will allow organizations to stay ahead of threat actors.

Risk-Appropriate Defense Programs

The vital intelligence received form an enhanced fraud risk assessment narrows the focus of risk response. With additional intelligence, governments can target medium to high priority fraud risks and place stronger guardrails to plug the gaps and weaknesses.

It is easier to set up a proper defense with in-depth intelligence. The key is to connect deep and dark web intelligence with the fight against threats to achieve a level of risk tolerable. Governments are faced with a multitude of threats from financial, non-financial, reputational, and national security related. Pools of intelligence are awaiting use to build a risk-appropriate defense program.



Dark Web Case Study #1

Overview

The public sector client selected a contractor to pilot a project to **monitor the dark web and identify Medicare** related fraud schemes. The objective was to help the client determine if full implementation of a dark web monitoring program would be useful.

Key Insights & Outcomes from the Pilot

Getting the details. The pilot showcased that identifying compromised information was only the first step, but the challenge was in analyzing the intelligence to develop and execute a strategy to close the vulnerability.

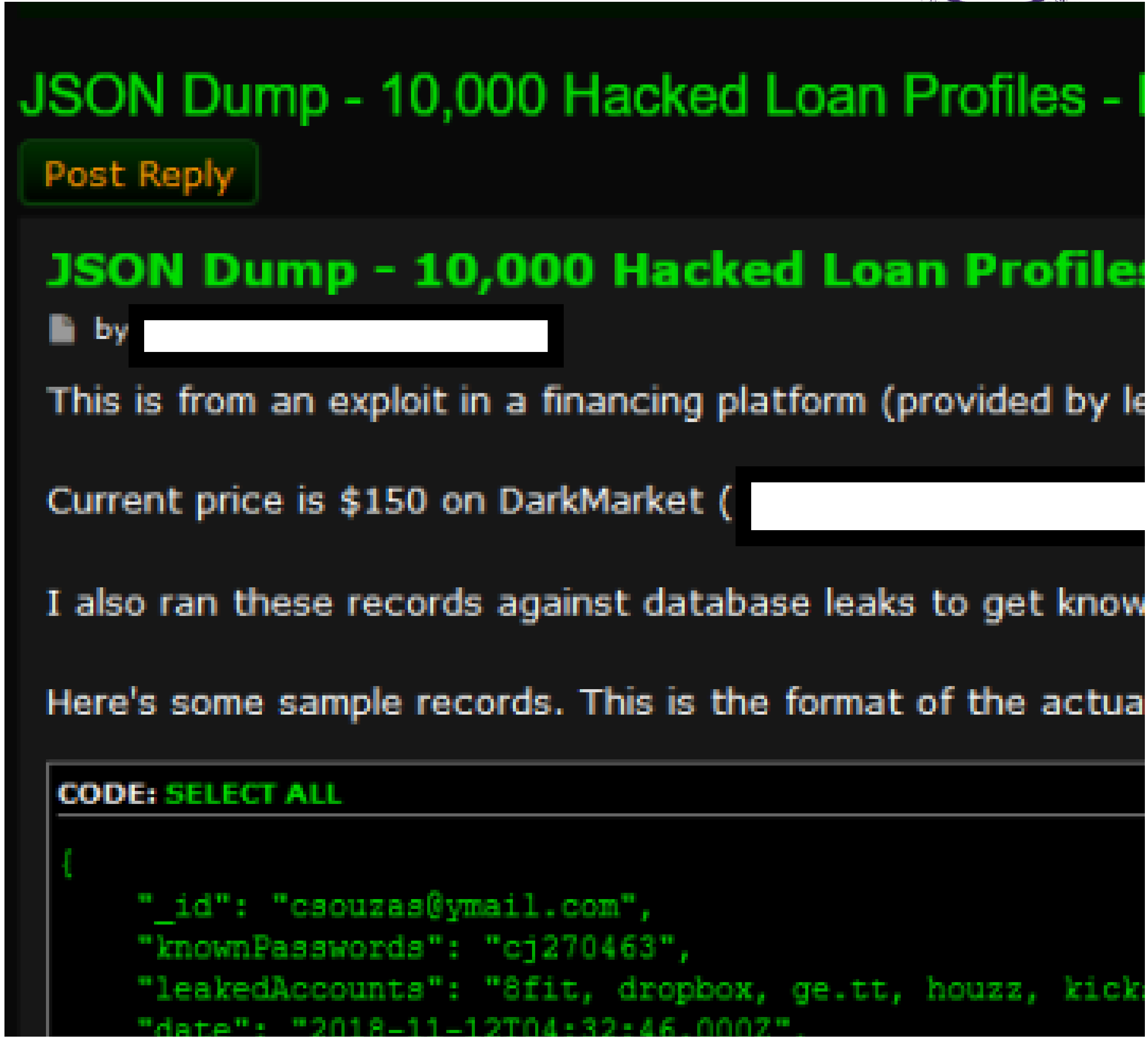
Taking action. An administrative priority for the client is facilitating take-downs through partnerships with law enforcement. However, the dark web analysis produced during the pilot did not lead to credible intelligence for the client's law enforcement partners to act against fraudsters. This left the client with few options to take administrative action against the potential fraudsters.

Dark Web Case Study #2

Risk: Stolen Information for Sale – Identity Theft

Problem: This showcases a real-world example of a fraudster selling compromised information on the dark web.

Resolution: You can identify compromised information – such as financial information – and **collaborate with the necessary stakeholders within your organization to notify victims and issue new credentials** as part of risk response. Your organization could target reviews for claims associated with compromised or stolen information.



JSON Dump - 10,000 Hacked Loan Profiles - I

JSON Dump - 10,000 Hacked Loan Profile

by [redacted]

This is from an exploit in a financing platform (provided by le

Current price is $150 on DarkMarket ([redacted]

I also ran these records against database leaks to get know

Here's some sample records. This is the format of the actua

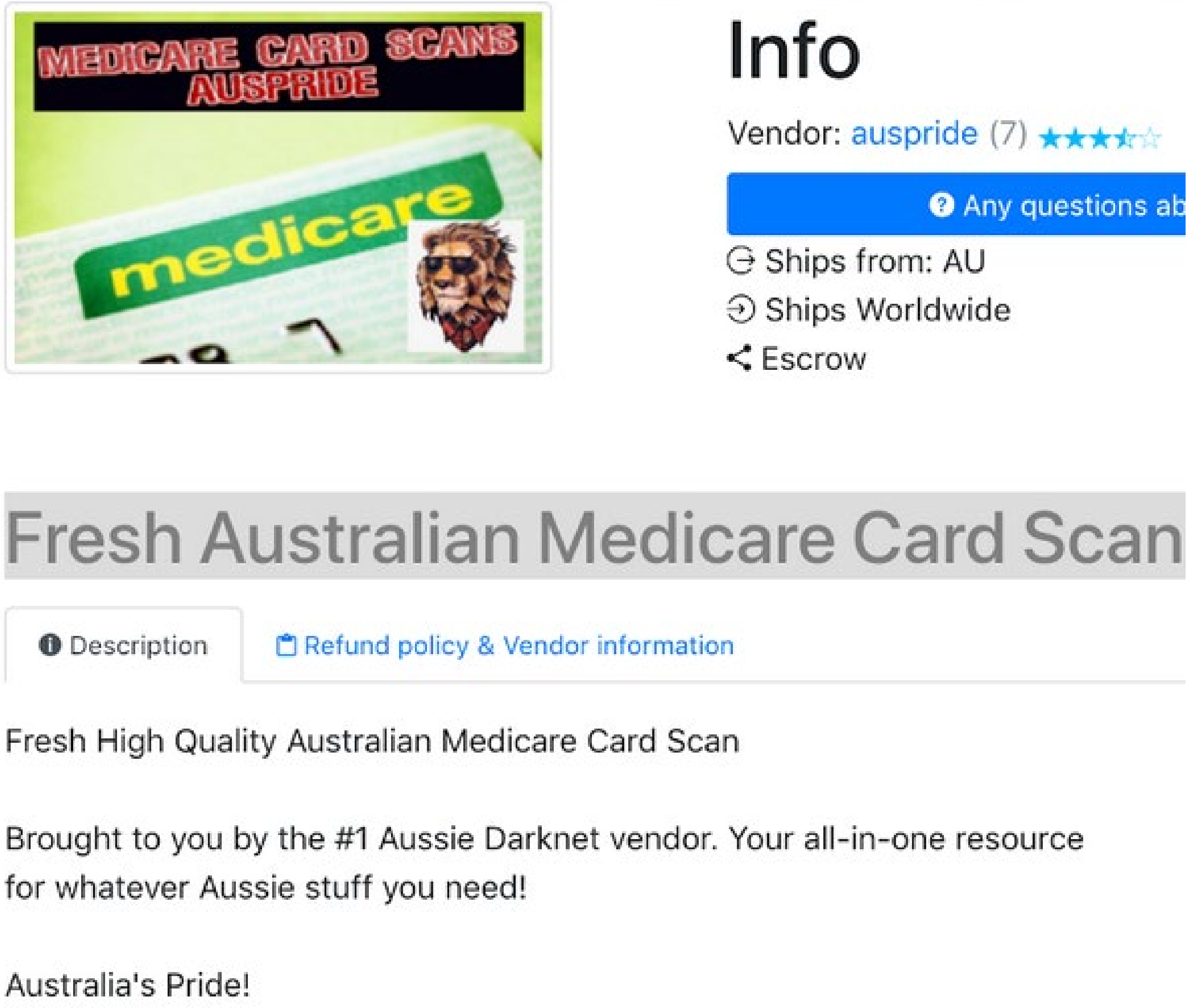
```
{
    "_id": "csouzas@ymail.com",
    "knownPasswords": "cj270463",
    "leakedAccounts": "8fit, dropbox, ge.tt, houzz, kick
    "date": "2018-11-12T04:32:46.000Z",
```

Dark Web Case Study #3

Risk: Stolen Information for Sale – Identity Theft

Problem: This showcases a real-world example of a fraudster selling fake Medicare cards and credentials.

Resolution: Your organization **can collaborate to enhance beneficiary enrollment controls and determine mechanisms to increase awareness of fraudulent cards across the provider population to ensure providers know how to spot fake cards and/or credentials.** Further, you could target reviews for claims associated with fake credentials.



Info

Vendor: auspride (7) ★★★★☆

❓ Any questions ab

Ships from: AU

Ships Worldwide

Escrow

Fresh Australian Medicare Card Scan

Description | Refund policy & Vendor information

Fresh High Quality Australian Medicare Card Scan

Brought to you by the #1 Aussie Darknet vendor. Your all-in-one resource for whatever Aussie stuff you need!

Australia's Pride!

Reactive Approaches to Combat Fraud

The best defense is a good offense

Incident Response (IR)

Integrating incident response protocols into an organization’s overall cybersecurity policy and risk-mitigation strategy is both more efficient and cost-effective. A forensic investigator’s perspective on existing policies can help mitigate the damage of cybersecurity incidents by bringing a world-class incident response capability to address incidents when they occur.

- **Forensic investigations**
- **IR program development**
- **Capabilities assessment**
- **Cyber insurance reviews**
- **End-point detection and monitoring**
- **Organizational reporting**

Digital Forensics

A branch of forensic science focused on recovery and investigation of artifacts found on digital devices

- **Computer forensics** provides tools to collect and preserve legally admissible evidence from one or more computing devices.
- Once data is collected, can apply data mining and analytic techniques to extract and identify patterns and relationships within structured and unstructured data. Can be used in conjunction with data mining, E-discovery, threat hunting, and link analysis to discover and evaluate relationships and information for fraud investigations
  - Examples of data gleaned from digital forensics: location data, messages sent and received, photos
- Use cases: financial fraud investigations, cyber crimes (breaches, security lapse)

Any final questions?

FRAUD

PREVENT | DETECT | INVESTIGATE | @Grant Thornton

Q & A

Speakers

James Ruotolo

Senior Manager
Fraud & Financial Crimes
james.ruotolo@us.gt.com
@jdruotolo

Taylor Larimore

Senior Manager
Fraud & Financial Crimes
taylor.larimore@us.gt.com