2025 Fraud Landscape

American Bankers Association
NDBA
Monday, October 20, 2025

Top Fraud Risks

Fraud is everyone's concern, inside and outside of the bank's walls. I will provide an overview of critical risk area including imposter scams, Identity Theft, account takeover (ATO) fraud, check fraud and more.

American Bankers Association®

Fraud Trends

70%

Of businesses report that fraud losses have increased in recent years and over half of consumers feel they are more exposed to fraud than a year ago

22%

A 2025 report found that fraud on **P2P platforms** had increased 22% and was 1 of the 6 most common types of fraud

CHECK FRAUD

2024, FinCEN received 682,276 SARs related to check fraud from depository institutions, up once again

64%

of consumers now say they are concerned somewhat concerned about online fraud

IMPOSTER SCAMS

1 in 3 people lost money to scams, with a reported loss of $12.5 Billion (up $2.5B from 2023)

Younger people lost money money more often

But when older adults reported losing money, money, they lost far more...(FTC)

Fraud Trends

Identity Theft

Remains one of the **most common** types of fraud, driving other fraud activity.

In 2024, identity theft accounted for 18% of all reports to the FTC's [Consumer Sentinel Network](), which was 1.1 million reports. This was the second most common category, following fraud (40%)

Phishing Attacks

Continue to be a **major threat**, #1 reported complaint to FBI IC3

Email is the highest attack vector, with 372,00 reported to the FTC

While social media contact has the highest loss associated to it , at $1.9B

Account Takeover (ATO)

Increased by 23% in the last year, with **account opening fraud close behind**.

Account takeover fraud cost US adults roughly $15.6 billion in 2024, a 23% increase from the previous year.

ATM Bitcoin

FTC says that fraud losses to Bitcoin ATMs have topped $1.4 billion in 2024

Synthetic Identity Fraud

Losses projected to reach over **$2.5 billion in 2023.**

Fraud Trends

Social media tends to be the most effective communication method for defrauding consumers… Most of these contacts led to investment scams for the largest total financial losses overall in 2024, with $5.7 billion lost.

By comparison, **email** had the least effective method of communication for stealing from consumers; **the median financial loss reported was $600**

- ❖ The most effective scams for producing a financial loss often rely on a blend of email and other channels, like follow-up phone calls or social media, which may obscure the exact percentage for email alone.

Current Fraud Tactics

Automation & Generative AI

Enabler for fraudsters, specifically making it more accessible to do-it-yourself

Synthetic Fraud / Rise of Synthetic Identities

Adoption of new digital payments & methods

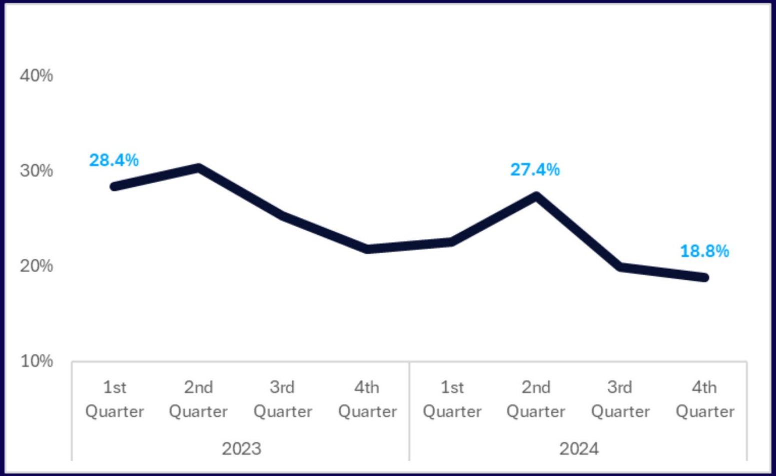
Online account opening/ACH & Wire automation

Money Mule Schemes

Fraudsters (Money Mules) are Beating Banks at Account Opening

auriemma roundtables

Rate of New Accounts Declined at Application

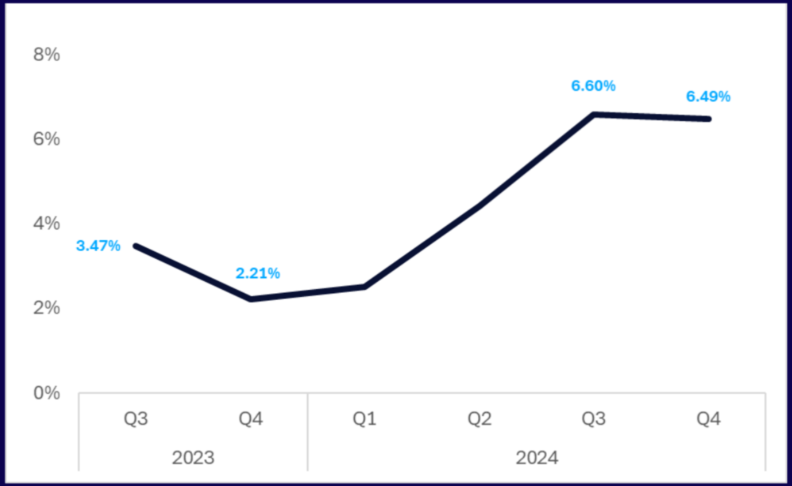


Source: Auriemma Roundtables benchmark data

Find Out More:
www.roundtables.us

auriemma roundtables

New Accounts Closed After Opening for Fraud (%)



Source: Auriemma Roundtables benchmark data

Find Out More:
www.roundtables.us

Synthetic Identities are Driving Account Opening Fraud, Leading to Credit Fraud & Money Mules, at Scale

Traditional SID - Credit Fraud

- Still one of the fastest-growing financial crimes, with losses reaching $3.2 billion in early 2024, up from $3 billion in 2023
- Credit and lending products
- Credit Card process used to pollinate synthetics at scale
  - Springboard to other credit offerings in bank

Modern SID – Money Mules

- Fraudsters exploit gaps in identity verification, creating fabricated identities that bypass traditional detection methods
- CYBERA/FS-ISAC partnership, identified 5 largest money mule rings funneling scam proceeds thru 610 transactions across 535 bank accounts over 8 months
  - While these five rings account for just 3% of the unmasked mule herders, they collectively control **9%** of the **approximately 6,000 money mules accounts sitting** in the top 10 US banks, alone

CHECK FRAUD IN 2024

The 2024 AFP Payments Fraud and Control Survey listed checks as the payment method most vulnerable to fraud.

70%

The 2024 AFP Payments Fraud and Control Survey reported that, despite the high resurgence of check fraud, 70% of organizations currently using checks do not plan to discontinue their use.

Mail Theft Impact

Mail theft is a significant contributor to the rise in check fraud. In 2018, the USPS reported 80 robberies. In the first half of 2023, the USPS reported 717 robberies.

In 2023, one institution reported $135 million in losses due solely to check fraud

Fraud Detection Challenges

There will likely be a continued increase in first-party fraud

1. Via people voluntarily acting as as mules for criminal networks for networks for a share of the proceeds

2. As the shift in liability for fraudulent payments more prevalent

The level of sophistication will only grow as fraudsters look to leverage these sophisticated tools.

Deep Fakes, Voice cloning, and manipulation of photos, as AI will be leveraged by Fraudster carry out their attacks.

More consumers are looking to in-person interactions to reduce

Fraud Detection Challenges

Key Issues

Increase in FinTech Relationships

Balancing "Friction" and "Fraud Mitigation" becomes even more challenging as the number of number of systems increases.

Good Controls in place related to scams

Cost of Frauds

Surge in Synthetic ID Fraud

Approaches & Proactive Solutions

Fraud Fusion Strategy

Multi-Layered Fraud Assessment

Real Time Risk Assessment

Getting Ahead of Fraud Trends (Go on Offense)

How to Combat Fraud?

- Data Encryption & Security
- Advanced Authentication Methods
- Customer Education & Awareness
- Artificial Intelligence & Machine Learning
- SMART Investment in Technology
- Enhanced Identity Verification
- Incident Response & Recovery
- Real Time Monitoring, Alerts, & Info Sharing
- Behavioral Metrics

What is the one thing below that you feel would better help your bank protect customers from fraud?

01 Better technology

02 Stronger safe harbor laws for info sharing sharing

03 Clarity from regulatory bodies enforcing applicable regulations

04 Universal hold harmless / indemnification

05 Standardized processes for incoming fraud / unauthorized payment notifications

Contact Information

Jim Hitchcock

VP, Fraud Mitigation

American Bankers Association

jhitchcock@aba.com

Appendix

- ABA Fraud Resource 1-Pager
- ABA Fraud Indicator eXchange (FIX) Pending Project
- UK Stop, Hang Up,Call – Stop Scams Initiative
- Case Studies
  - Business Check Fraud
  - Job Scam

ABA Fraud Resource Page

ABA.com/fraud

To find out if your bank is an ABA member, or to learn more about becoming one, visit:

ABA.com/membership

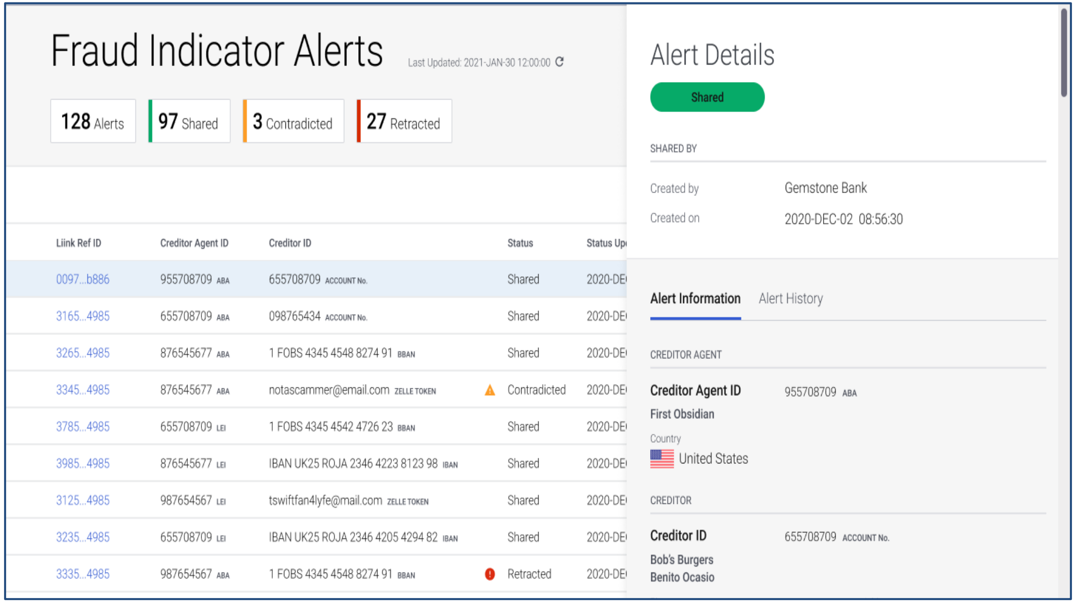
ABA Committees, Councils and Working Groups.
Learn more at: **ABA.com/experts-peers/committees-councils**

Some of ABA Fraud Resources Include:

- **ABA Fraud and Scams Exchange**
- **ABA Fraud Contact Directory**
- **ABA Treasury Payee Verification**
- **ABA Fraudcast**
- **ABA Check Fraud Toolkit**
- **ABA Frontline Training Course on Check Fraud**
- **Banks Never Ask That & Practice Safe Checks**
- **ABA Check Fraud Product Assessment**
- **ABA Compliance Hotline**
- ***Learn more at ABA.com/Fraud***

Questions? Email fraud@aba.com

ABA Fraud Indicator eXchange (Project Temporarily on Hold)



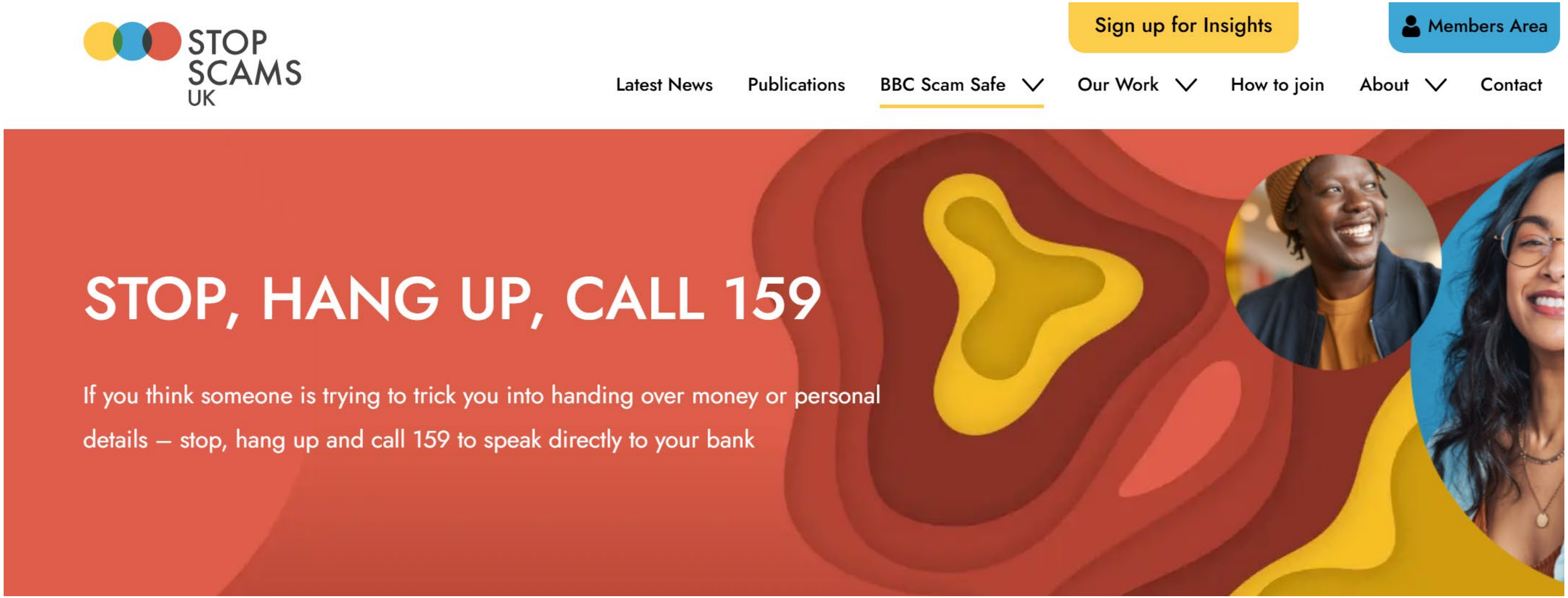
Current State:

A fraudster can successfully attack victims across various banks, exploiting **delays in account closures** and **gaps in information sharing** across the industry.

Future State with Data Sharing:

The first bank to identify indicators of fraud **alerts the industry** to help other **banks avert losses for subsequent victims** until the fraudulent account is closed.

STOP, HANG UP, CALL 159 - Stop Scams UK



NEWS • PRESS RELEASES

D.A. Bragg: Check Fraud Ring Indicted For Stealing $1.2M From Bazooka Companies, Maker Of Classic Bubble Gum

OCTOBER 3, 2024

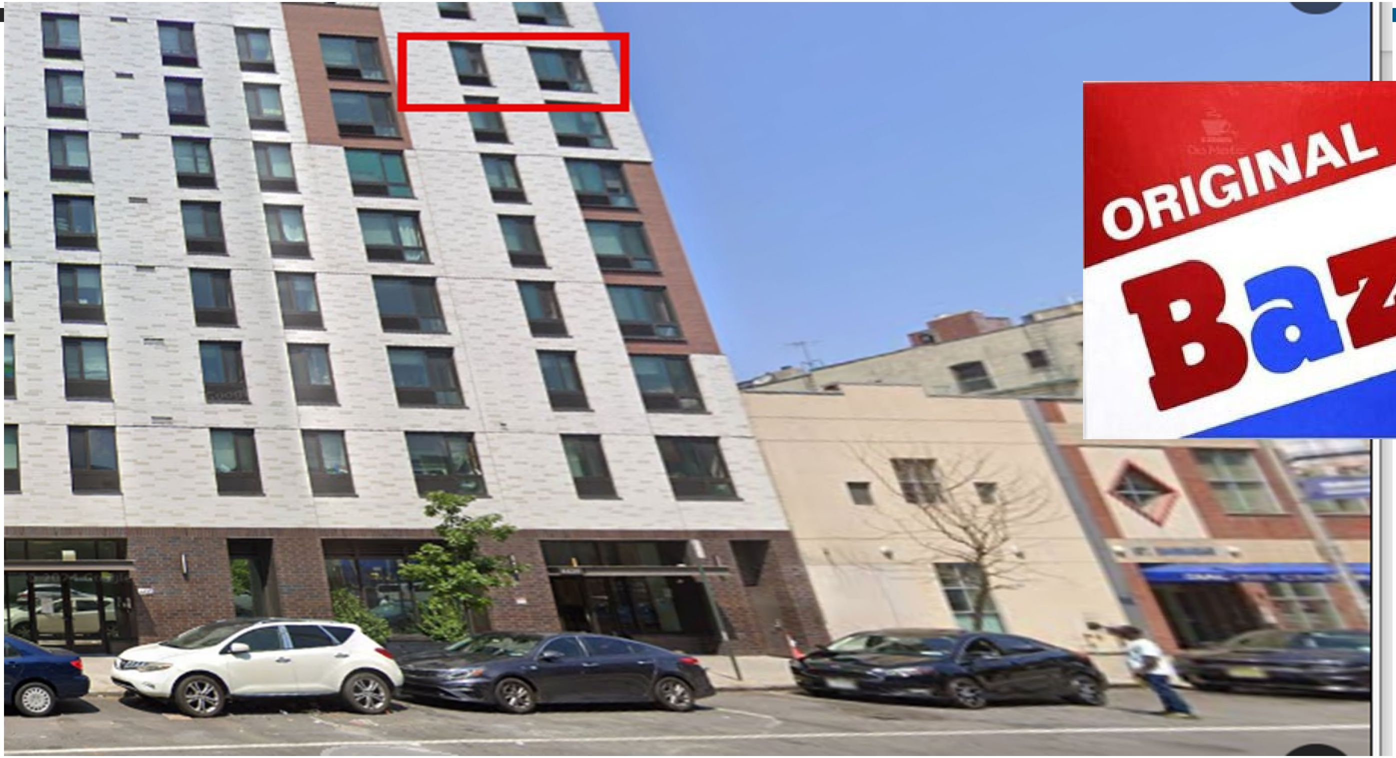
Manhattan District Attorney Alvin L. Bragg, Jr., today announced the indictment of KASHAWN WILLIAMS, 31, for intercepting a $1.2 million check intended for The Bazooka Companies Inc. ("Bazooka") and, alongside co-conspirators ADREAN JACOBS, 41, RONALD FRANKLIN, 49, JOSE GUTIERREZ, 25, AKHEIM WATTS, 30, and KIEARRA REYNOLDS, 35, laundering those stolen funds for personal use. The defendants are charged in a New York State Supreme Court indictment with Conspiracy in the Fourth Degree, Money Laundering in the First Degree, and Criminal Possession of Stolen Property in the First Degree, as well as various counts of Criminal Possession of Stolen Property in the Second Degree and Money Laundering in the Second and/or Third Degree. WILLIAMS is additionally charged with Grand Larceny in the First Degree and Identity Theft in the First Degree.[1]

"As alleged, this group stole more than a million dollars by intercepting a check, creating a fraudulent corporate business account, and laundering the money for personal gain," said District Attorney Bragg. "Despite the decline in the use of paper checks, check fraud is on the rise. We urge New Yorkers and businesses alike to use secure electronic payment methods whenever possible to protect themselves from fraud."

According to court documents and statements made on the record in court, in October 2022, WILLIAMS intercepted a $1,243,345.36 check mailed by a Texas-based company to a Manhattan address formerly associated with Bazooka, the creators of the Bazooka brand of bubble gum. On October 21, 2022, WILLIAMS incorporated a fictitious entity – The Bazooka Companies 1 Inc. ("Bazooka 1") – to serve as a conduit for the stolen proceeds. Three days later, WILLIAMS opened a corporate bank account for Bazooka 1 and deposited the stolen check.

Over the course of the next two weeks, WILLIAMS issued checks from the Bazooka 1 account to JACOBS, WATTS, GUTIERREZ, and REYNOLDS, listing fake reasons for the checks on their memo lines, such as "Renovations," "Business Loan," and "Packaging Preorder." The defendants then deposited these checks into their personal bank accounts and made large cash withdrawals.

Corporate Headquarters – KYC / KYB?



KYC Passed

https://apps.dos.ny.gov/publicInquiry/#search

Lastest Filing Information

Filing Number	221021003171
Filing Type	CERTIFICATE OF INCORPORATION
Mod Cert Code	01DB A
Approved Date	2022-10-21
Filing Date	2022-10-21
Entity Type	DOMESTIC BUSINESS CORPORATION
Current Entity Name	THE BAZOOKA COMPANIES 0 INC.
Effective Date	2022-10-21
Duration	PERPETUAL
Law Section	BUSINESS CORPORATION - 402 BUSINESS CORPORATION LAW
NFP Category	NO-ANSWER
County	Bronx
Jurisdiction	NY
Filer Name	KASHAWN WILLIAMS
Filer Address	4439 Third Avenue Apt 7e Bronx NY 10457-

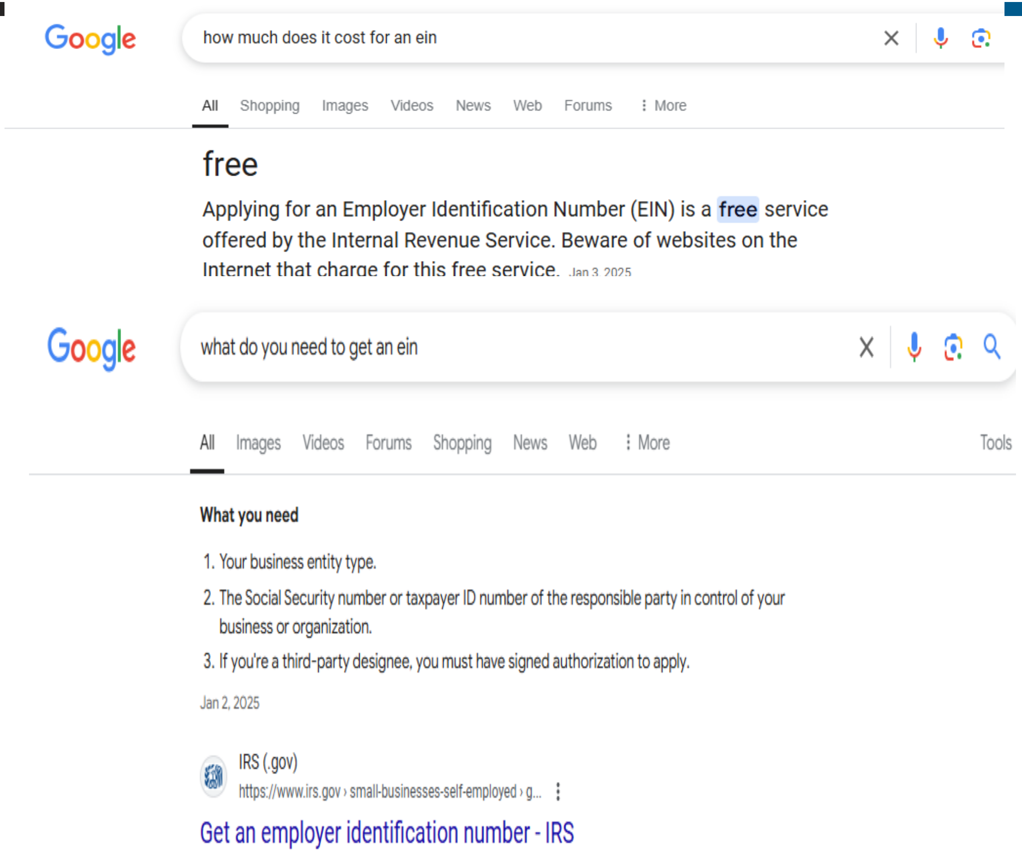
Business Entity Information

DOS ID	6621450
Current Entity Name	THE BAZOOKA COMPANIES 0 INC.
County	Bronx
Jurisdiction	New York
Entity Type	DOMESTIC BUSINESS CORPORATION
Initial DOS Filing Date	2022-10-21
DOS Process Name	Kashawn Williams
DOS Process Address	4439 Third Avenue Apt 7E Bronx NY 10457

Entity Name History

Filing Date	Entity Name	Filing Number	Type	Status
2022-10-21	THE BAZOOKA COMPANIES 0 INC.	221021003171	Actual	Active

EIN's are FREE- No Authentication Needed



Beating KYC Over Messaging App

Criminal 1: I'm ready for payment on corp.

Criminal 2: How much

Criminal 1: He's going to be the proud owner of [Entity Name] since Feb 2018; $550 includes DBA

Criminal 2: Okay I'll go to the bank in a few

Criminal 1: Do you have a blank EIN doc? Let's have it all ready so there is no question moving forward. I'll even give you a link to the state website so they can Verify everything online.

Criminal 2: Verify what? I typically just make a new one and photoshop the notice date and ein

College Job Scam

From: Bozena Michniak-Kohn <michniakkohnb@gmail.com>
Date: March 19, 2025 at 7:02:01 PM EDT
To: Michael <#####@Rutgers.com>
Subject: Re: Interdisciplinary Research Project Overview.

Stop, think…too good to be true?

Dear Michael,

We are excited to invite you to participate in an innovative, interdisciplinary research project that offers a unique opportunity to earn **$400 per week**. This project is designed to be flexible (**2-3 days per week**) and accessible (**Remote Work**), making it a perfect fit for those looking to balance work with other commitments.

If you're interested, we kindly request the following details to share further information:

- **Full Name**
- **Cell Phone Number**
- **Alternate Email Address**

Pause, what's wrong with this email? Why move to different one

Once we receive your information, kindly share the following details along with your updated ***resume*** for review:

- **Age:**
- **Bank Name:** (For timely paycheck processing)
- **Can you make a mobile deposit when your paycheck is sent?**

Really!

We look forward to your response!

Warm regards,

Bozena Michniak-Kohn
Professor of Pharmaceutics
Rutgers University–New Brunswick

Research source – Rutgers Pharmaceutics has endowment! So, sig block should include it