# Prime Match: A Privacy Preserving Inventory Matching System

Usenix Security 2023

Antigoni Polychroniadou

(J.P. Morgan AI Research & AlgoCRYPT CoE)

joint work with: Gilad Asharov (Bar Ilan University), Ben Diamond, Tucker Balch, Hans Buehler, Richard Hua, Suwen Gu,Gregory Gimler, Manuela Veloso

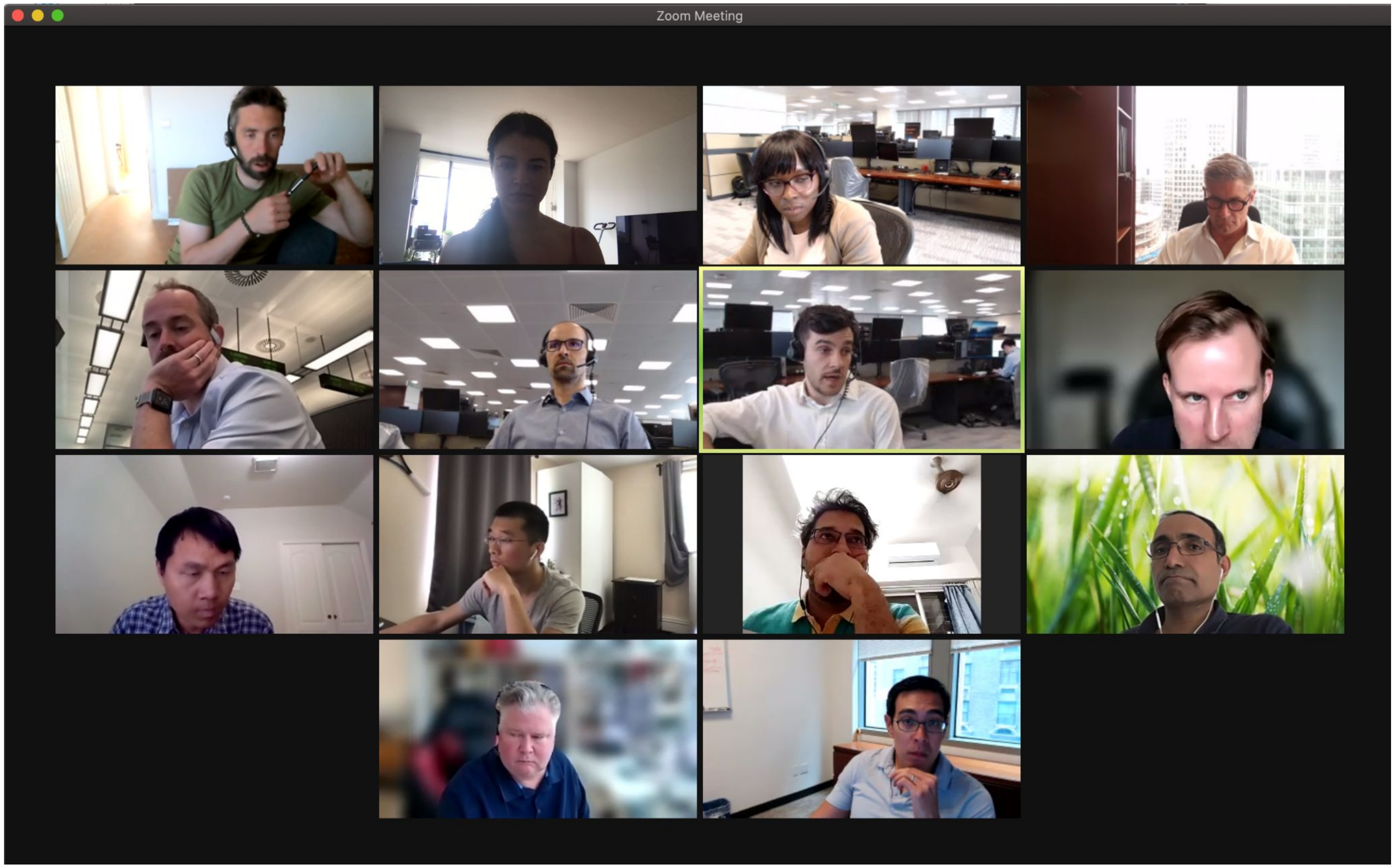
Markets of the Future

AlgoCRYPT CoE

AI Research

J.P.Morgan

# Prime Match: Extended Team



Mike Reich, Vaibhav Popat, Sitaraman Rajamani, Dan Stora, James Mcilveen, Oluwatoyin Aguiyi, Niall Campbell, Wanyi Jiang, Grant McKenzie, Steven Price, Vinay Gayakwad, Srikanth Veluvolu, Noel Peters and Jason Sippel

# Motivation

- First one-time application of MPC (electronic double auction): Sugar bit auction [Bogetof et al. 2008]
- MPC Dashboard

- Identify a real-world problem for MPC in the traditional financial world
- Academic work on privacy preserving darkpools [CSA19, B**P**V20, CSA20, MD**P**B23]
- Prime Match is the first MPC auction running live in the traditional financial world.

# Outline

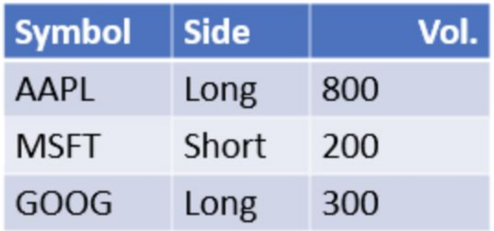
- Prime Match Problem Statement & Motivation
- Cryptographic Contributions in Prime Match
- From Proof of Concept (PoC) to Product
    - Pre-production and Production challenges
- Cryptographic Solution
- Demo

# Starting point: Inventory Matching **without** Privacy

## Inventory Matching Process:

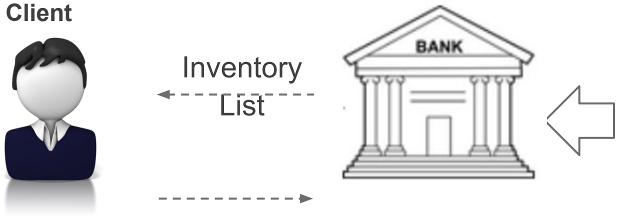
- **JPMC** Prime Brokerage desk **publishes daily** a list of inventory at a discount **to clients**
- Inventory includes a list of symbols, sides, volumes, rates for trades

Toy Inventory List Example:



| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | 800 |
| MSFT | Short | 200 |
| GOOG | Long | 300 |

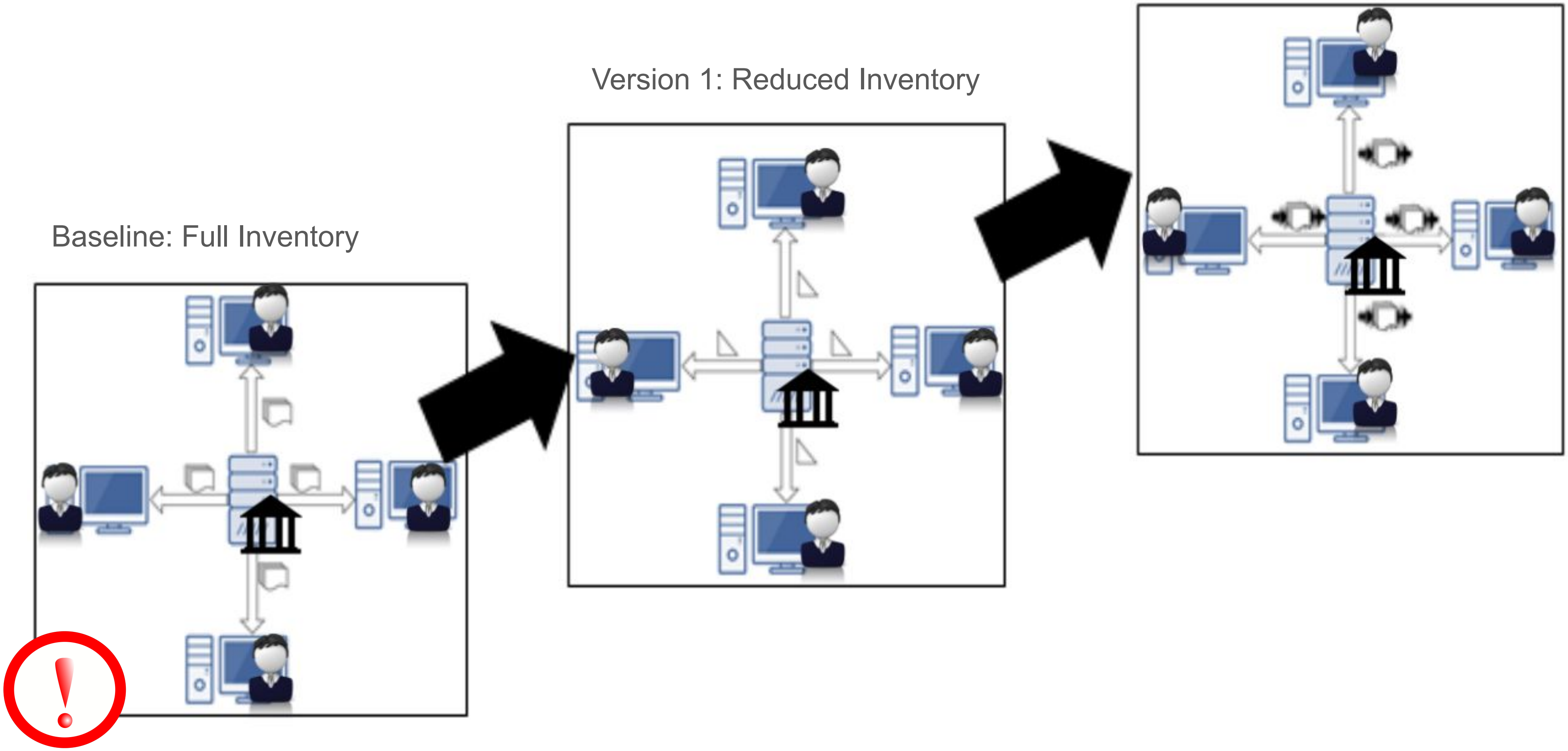
- JPMC processes **incoming trades** chosen from the list **by clients**



**Internal Data**

- JPMC inventory
- Financing rates
- Other firm / market data

# Starting point: Inventory Matching **without** Privacy



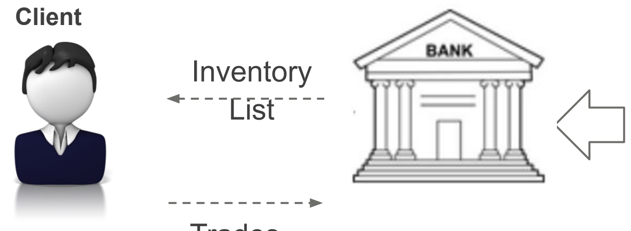
Baseline: Full Inventory

Version 1: Reduced Inventory

Version 2: Inventory with smart noise

# Starting point: Inventory Matching **without** Privacy

## Inventory Matching Process:



Client

Inventory List

Trades

BANK

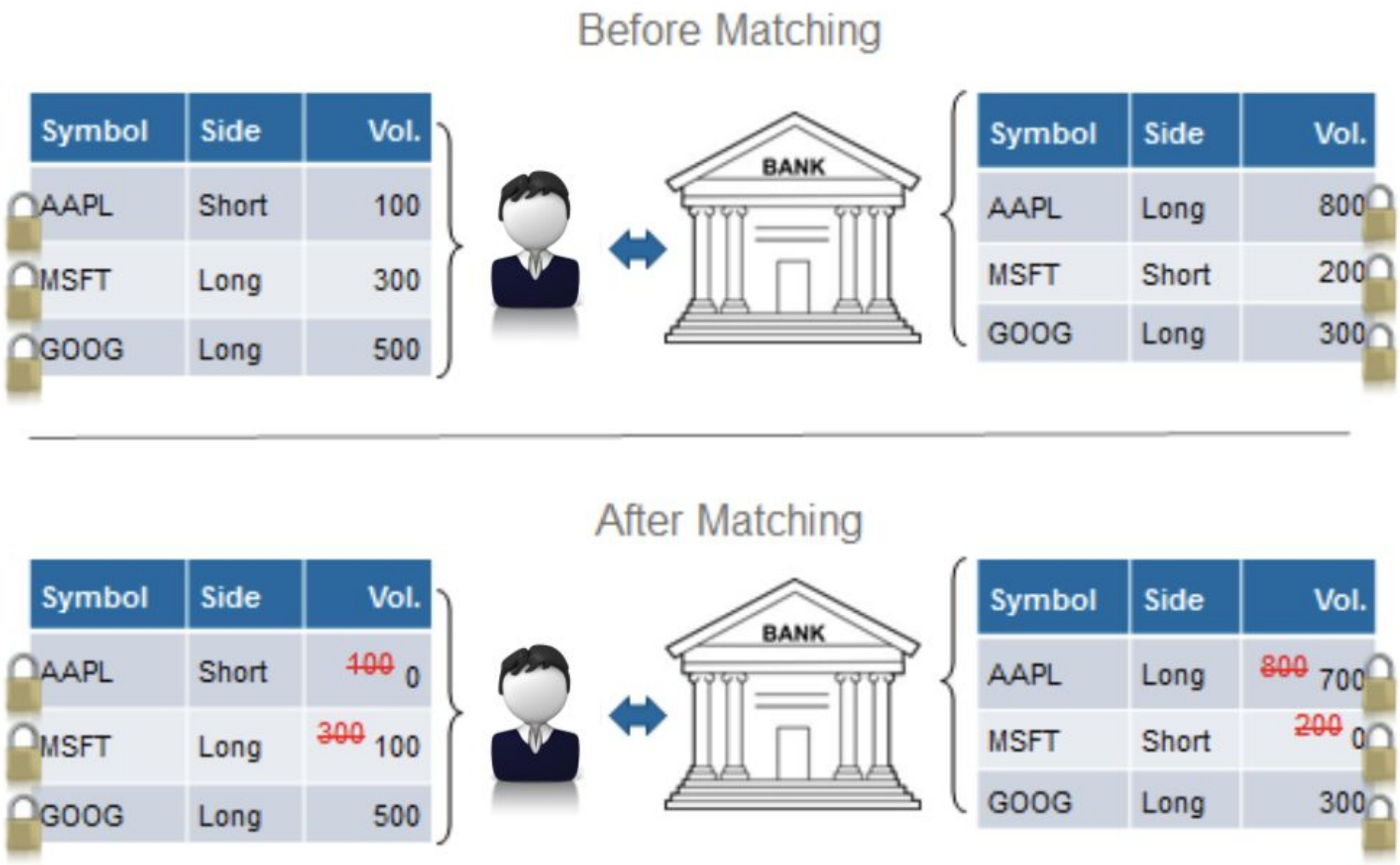
**Internal Data**

- JPMC inventory
- Financing rates
- Other firm / market data

## Problems with Inventory Matching:

- JPM reveals a large portion of its inventory list
- Clients raised concerns about potential leakage of their past trades included in the list
- Reduced inventory list available for matching
- Clients do not send to JPMC their inventory!

# Prime Match: Inventory Matching **with** Privacy



Before Matching

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Short | 100 |
| MSFT | Long | 300 |
| GOOG | Long | 500 |

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | 800 |
| MSFT | Short | 200 |
| GOOG | Long | 300 |

After Matching

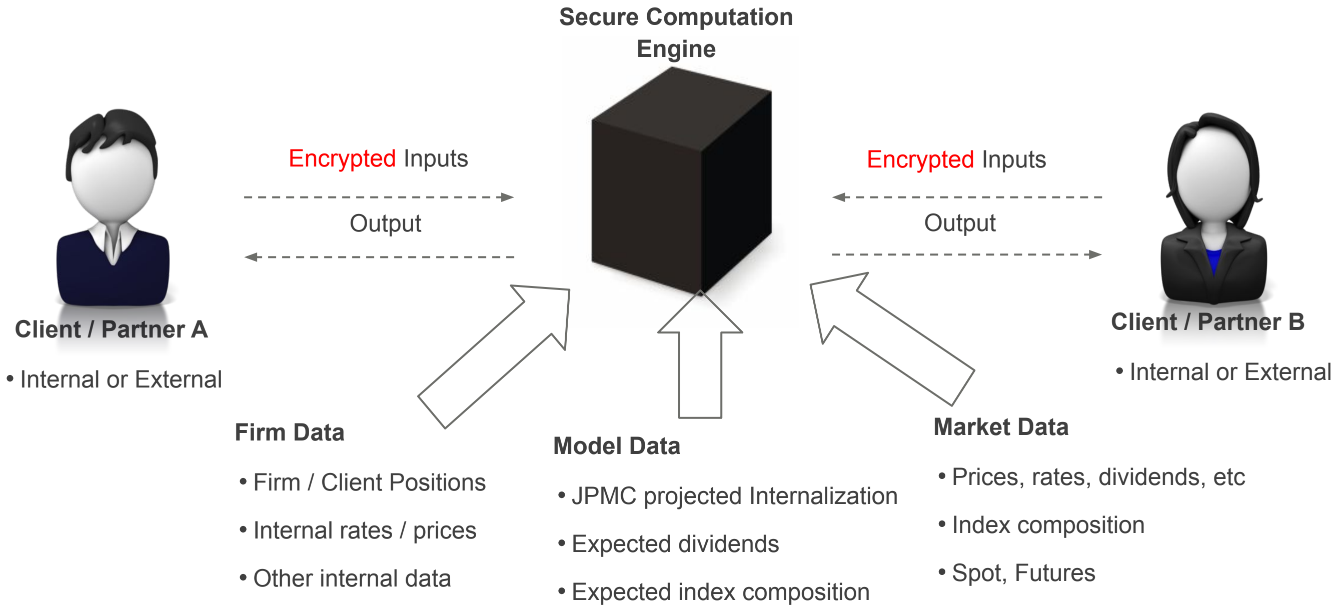
| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Short | ~~100~~ 0 |
| MSFT | Long | ~~300~~ 100 |
| GOOG | Long | 500 |

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | ~~800~~ 700 |
| MSFT | Short | ~~200~~ 0 |
| GOOG | Long | 300 |

Solution based on Secure Multiparty Computation

# Overview of Secure Multi-Party Computation (MPC)

- Enables different organizations / parties / entities to perform a joint computation over their inputs (i.e. trade lists) while keeping it private
- Encryption ≠ Secure Multiparty Computation:
  - Encryption: Parties trust each other, but do not trust some external that might eavesdrop to the conversation
  - Secure Computation: Parties do not trust each other or cannot share their data, but still want to compute on their joint private inputs
- **Feasibility** [Yao82,GMW87,BGW88,CCD88]: every distributed computation can be computed *privately*



**Secure Computation Engine**

Encrypted Inputs

Output

Encrypted Inputs

Output

**Client / Partner A**

- Internal or External

**Client / Partner B**

- Internal or External

**Firm Data**

- Firm / Client Positions
- Internal rates / prices
- Other internal data

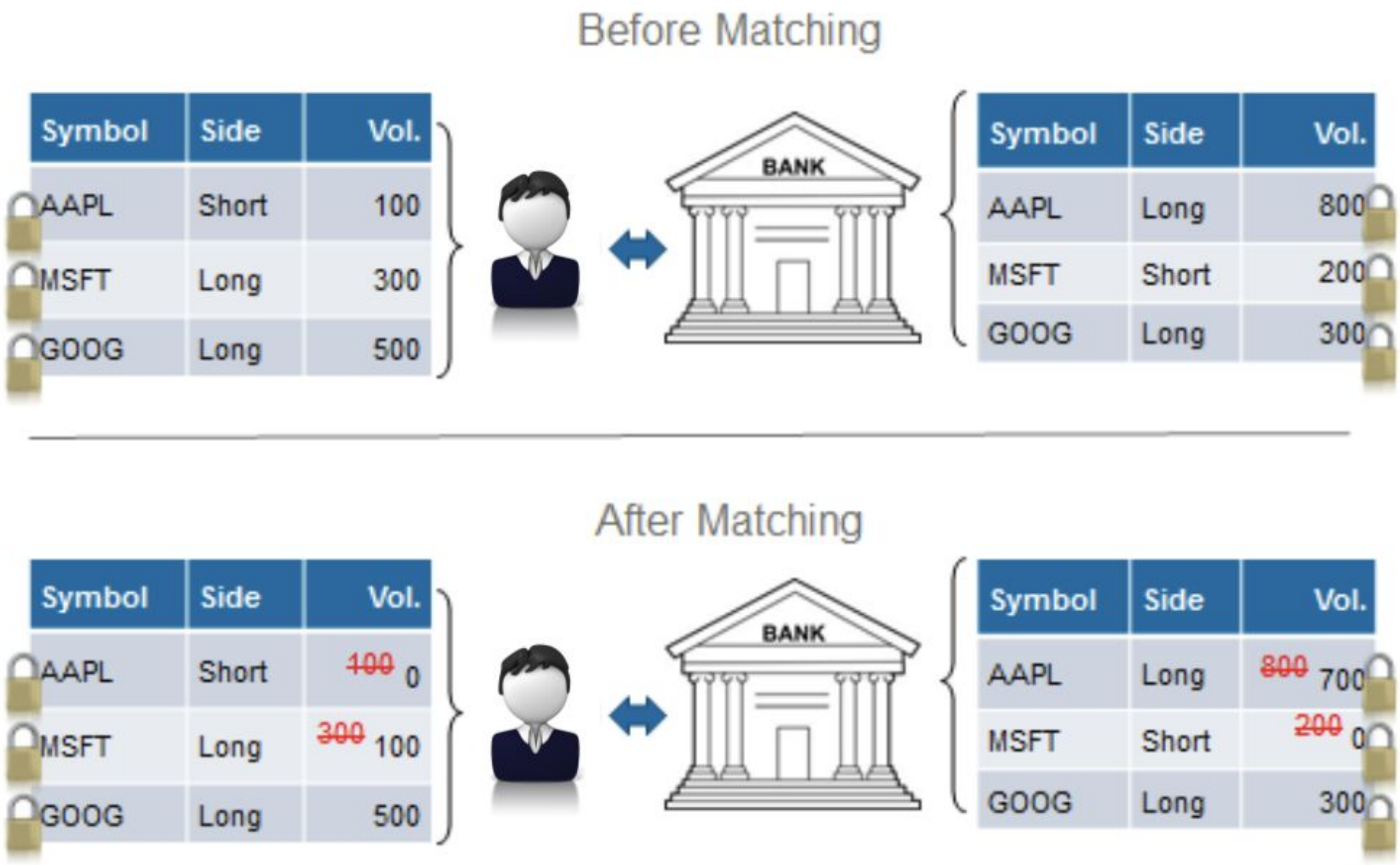
**Model Data**

- JPMC projected Internalization
- Expected dividends
- Expected index composition

**Market Data**

- Prices, rates, dividends, etc
- Index composition
- Spot, Futures

# Prime Match: Inventory Matching **with** Privacy



Before Matching

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Short | 100 |
| MSFT | Long | 300 |
| GOOG | Long | 500 |

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | 800 |
| MSFT | Short | 200 |
| GOOG | Long | 300 |

After Matching

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Short | ~~100~~ 0 |
| MSFT | Long | ~~300~~ 100 |
| GOOG | Long | 500 |

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | ~~800~~ 700 |
| MSFT | Short | ~~200~~ 0 |
| GOOG | Long | 300 |

**Main ingredient:** New secure comparison protocol for computing the minimum between two values such as min(100,800)

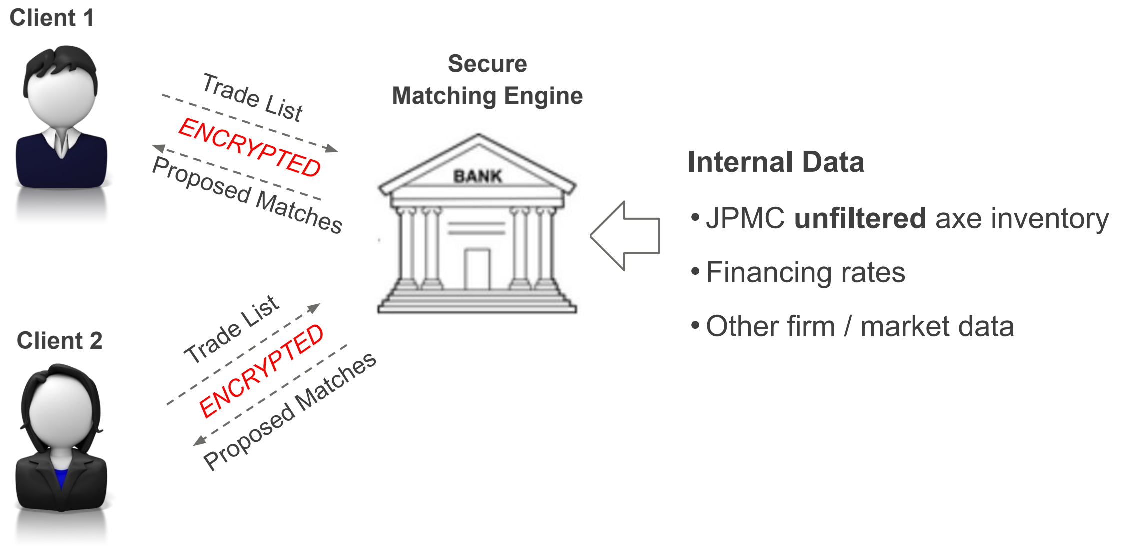
# Prime Match: Privacy-Preserving Inventory Matching with 2PC

## Proposed Service (via Secure Two-Party Computation)

- Client sends over their encrypted trade list
- Secure engine provides list of matching trades against its *full* inventory list

## Benefits:

- More tailored trades matching exact needs of clients; increased inventory availability
- JPM is not exposed to client's trade list unless there is a match; privacy is preserved:
  - No risk of information leakage to JPMC.
  - Unmatched positions are not revealed.



**Internal Data**

- JPMC **unfiltered** axe inventory
- Financing rates
- Other firm / market data

# Prime Match: Privacy-Preserving Inventory Matching with MPC

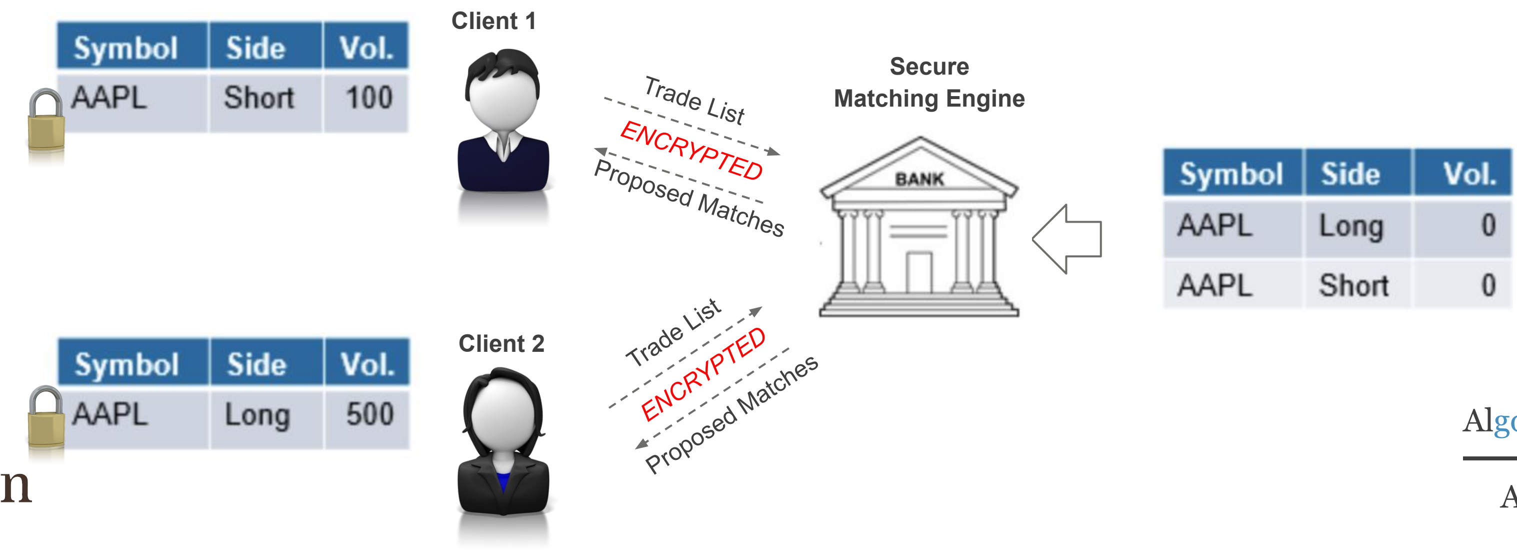
## Proposed Service (via Secure Multi-Party Computation)

- Client sends over their encrypted trade list
- Secure engine provides list of matching trades against its *full* inventory list
- Support provided to match trades **against other clients**

## Benefits:

- More tailored trades matching exact needs of clients with the ability to internalize across **multiple clients**; **significantly increased inventory** availability
- JPM is not exposed to client's trade list unless there is a match; privacy is preserved:
  - No risk of information leakage to JPMC.
  - No risk of information leakage to other clients.
  - Unmatched positions are not revealed.

Toy Example:



Client 1

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Short | 100 |

Client 2

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | 500 |

Secure Matching Engine

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | 0 |
| AAPL | Short | 0 |

J.P.Morgan

AlgoCRYPT CoE

AI Research

# Prime Match: Privacy-Preserving Inventory Matching with MPC

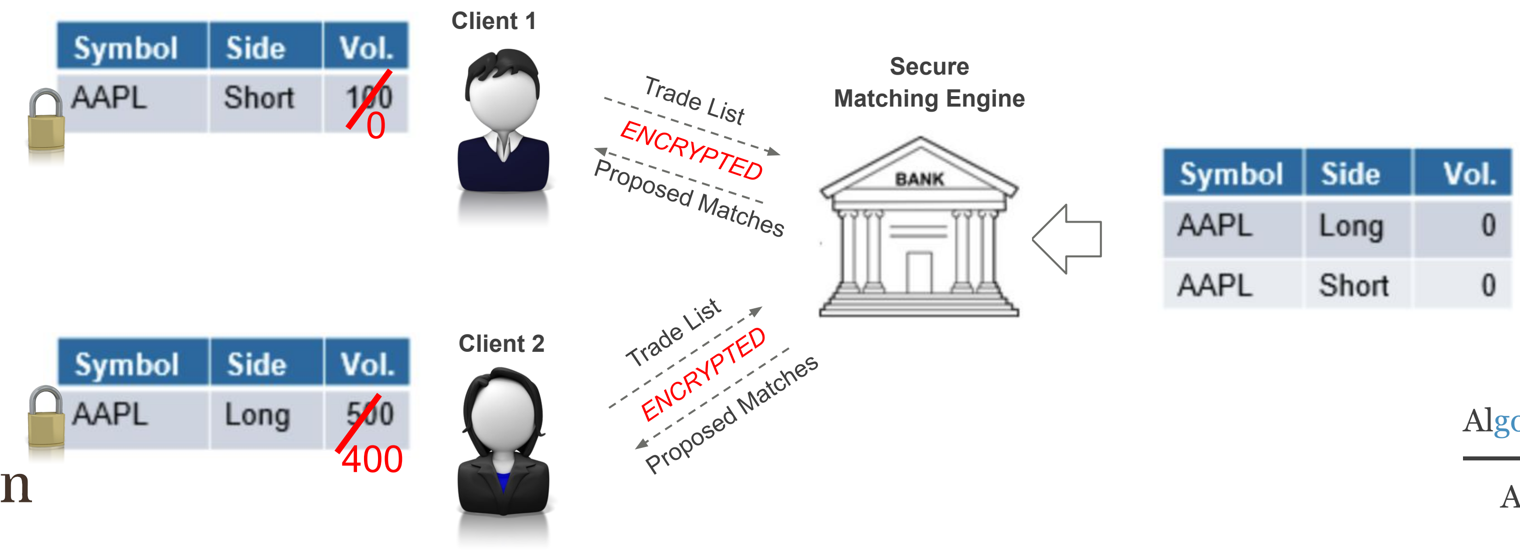
## Proposed Service (via Secure Multi-Party Computation)

- Client sends over their encrypted trade list
- Secure engine provides list of matching trades against its *full* inventory list
- Support provided to match trades **against other clients**

## Benefits:

- More tailored trades matching exact needs of clients with the ability to internalize across **multiple clients**; **significantly increased inventory** availability
- JPM is not exposed to client's trade list unless there is a match; privacy is preserved:
  - No risk of information leakage to JPMC.
  - No risk of information leakage to other clients.
  - Unmatched positions are not revealed.

Toy Example:



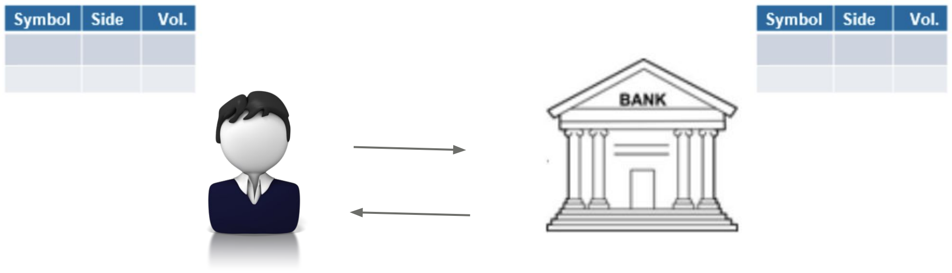
| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Short | ~~100~~ 0 |

| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | ~~500~~ 400 |

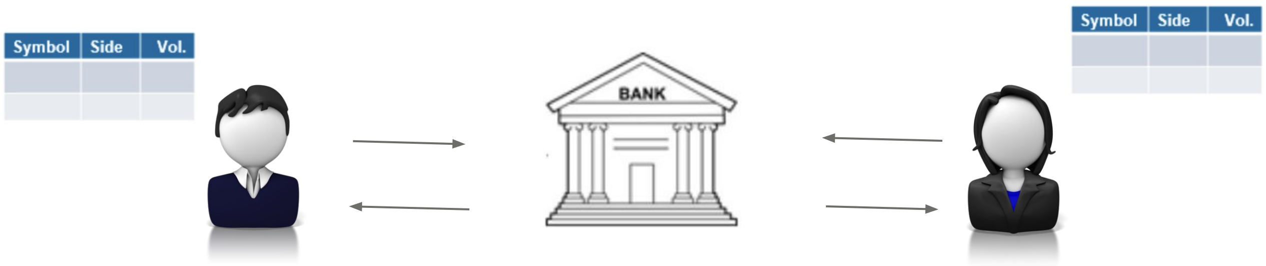
| Symbol | Side | Vol. |
|---|---|---|
| AAPL | Long | 0 |
| AAPL | Short | 0 |

# Cryptographic Contributions in Prime Match

Two-Party Secure comparison:



Three-Party Secure comparison with a third party acting as the facilitator:



New **two-round** secure **linear** comparison protocol for computing the minimum between two values with o**ne malicious corruption; no preprocessing**

Prior works: non-linear; log #round

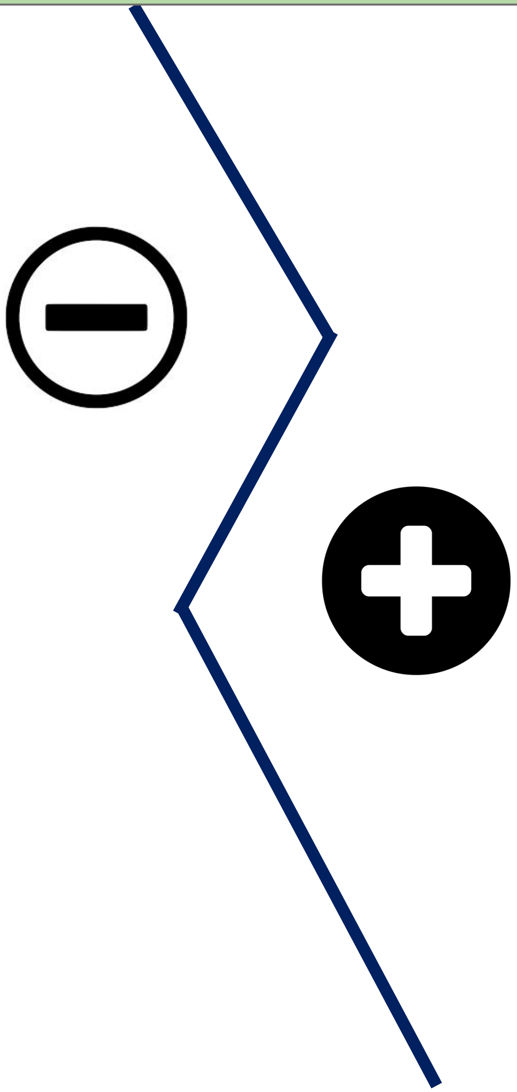
Improved version of SecureNN [WaghGuptaChandran19]

# Prime Match: Pre Production and Production challenges

# Prime Match: Pre-Production Challenges

2019

**No financial institution had taken the initiative to implement privacy preserving auctions**



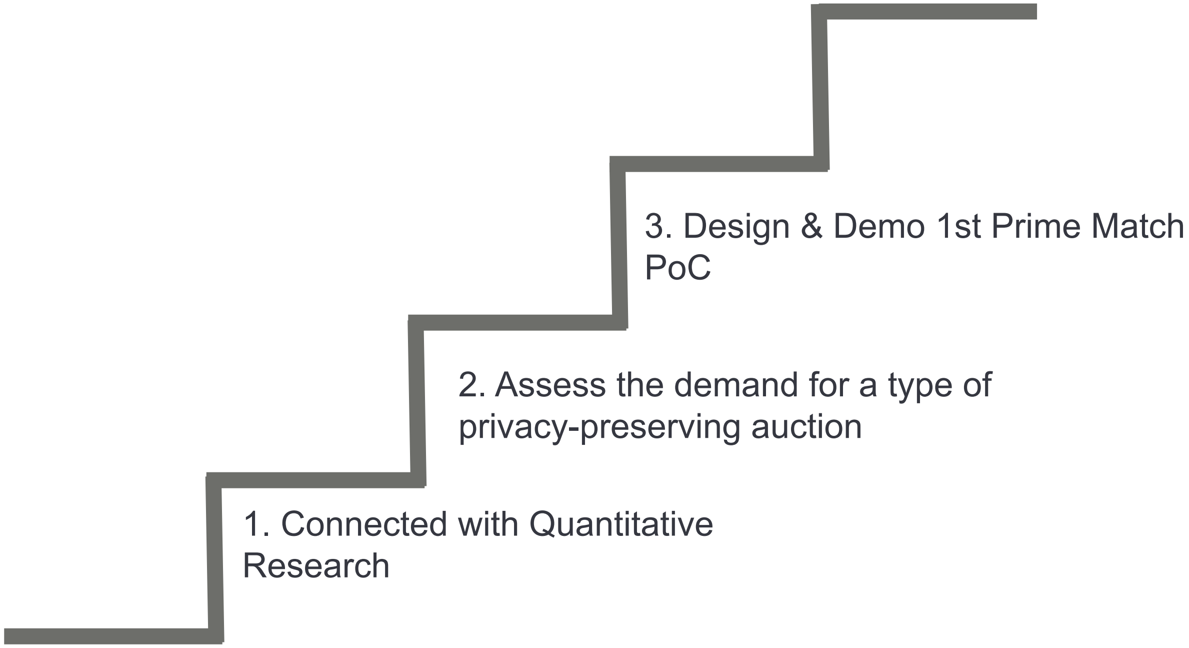
Prior to Prime Match,
**No** financial institution had
ever utilized Multi-Party
Computation (MPC)
technology.

The bank **has** long-standing clients

# Prime Match: Proof of Concept (PoC) Challenges

2019

**Internal buy-in to the product**



1. Connected with Quantitative Research

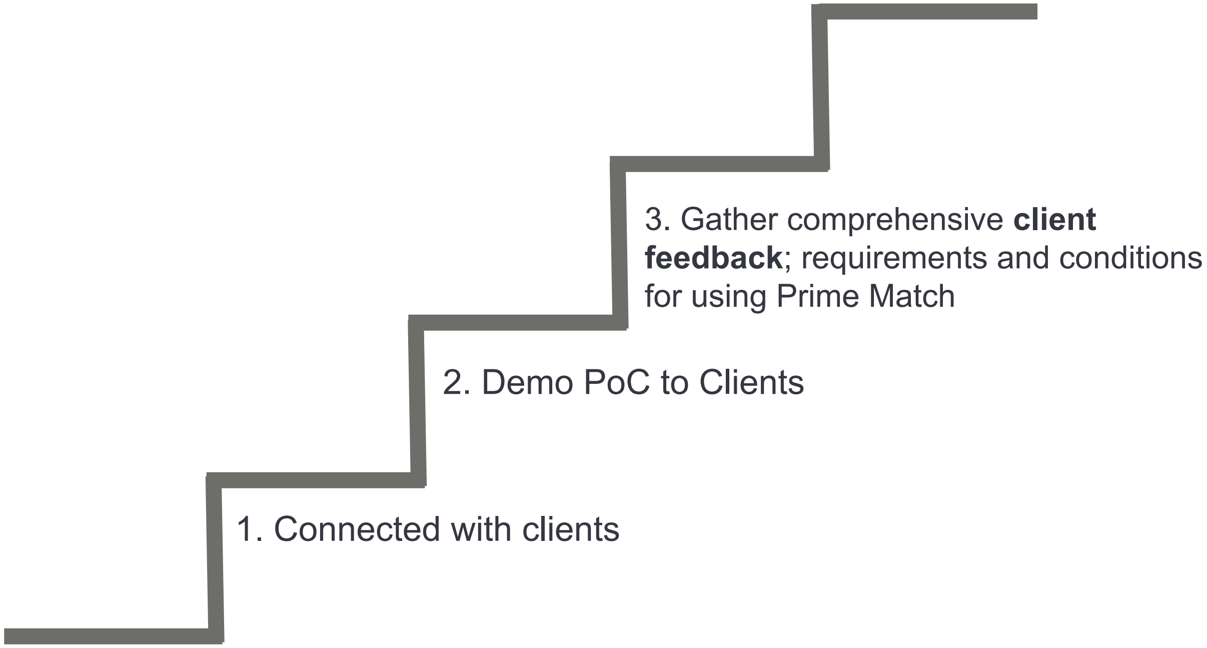
2. Assess the demand for a type of privacy-preserving auction

3. Design & Demo 1st Prime Match PoC

# Prime Match: Pre-Production Challenges

2020

**External buy-in to the product**



1. Connected with clients

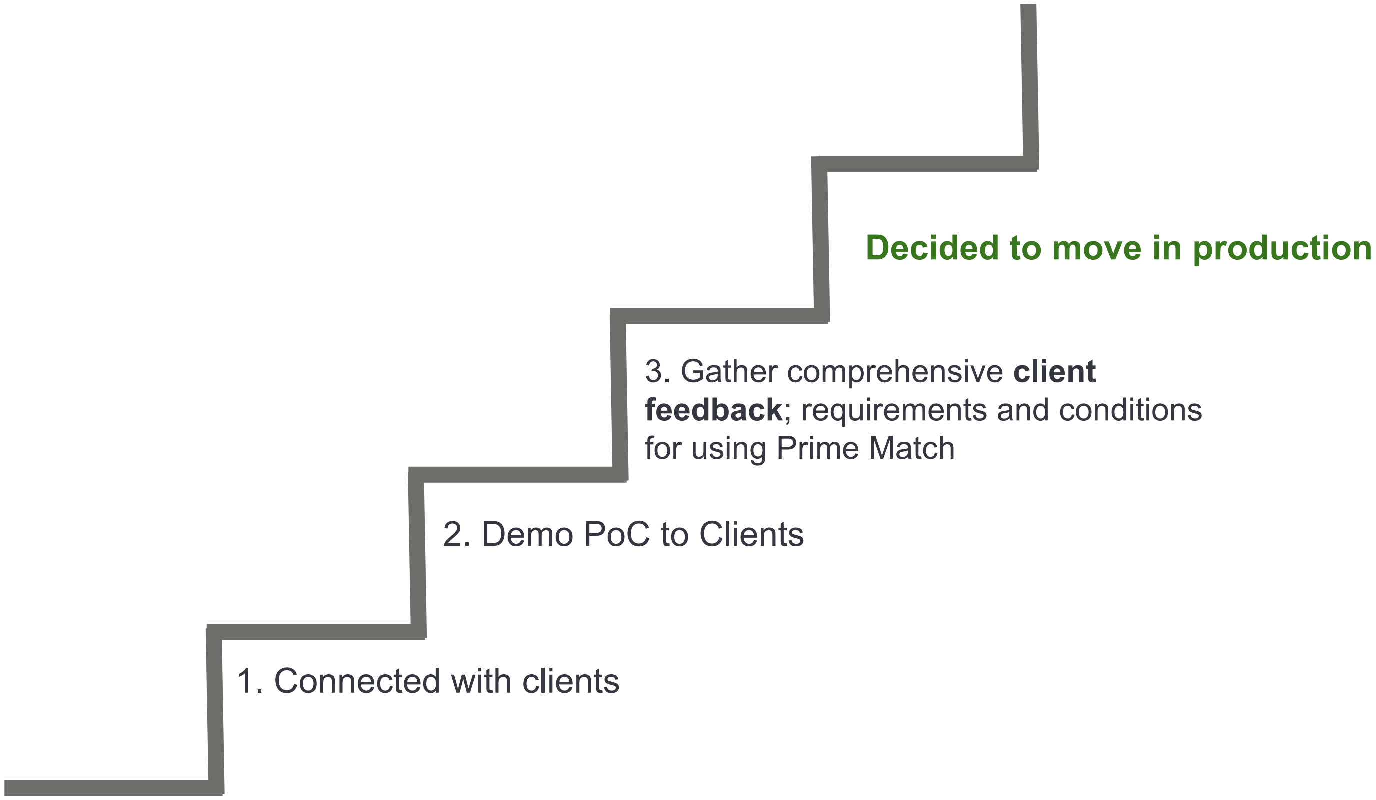
2. Demo PoC to Clients

3. Gather comprehensive **client feedback**; requirements and conditions for using Prime Match

# Prime Match: Pre-Production Challenges

2020

**Given the innovative nature of the product, the green light for production was given after a long process**



1. Connected with clients

2. Demo PoC to Clients

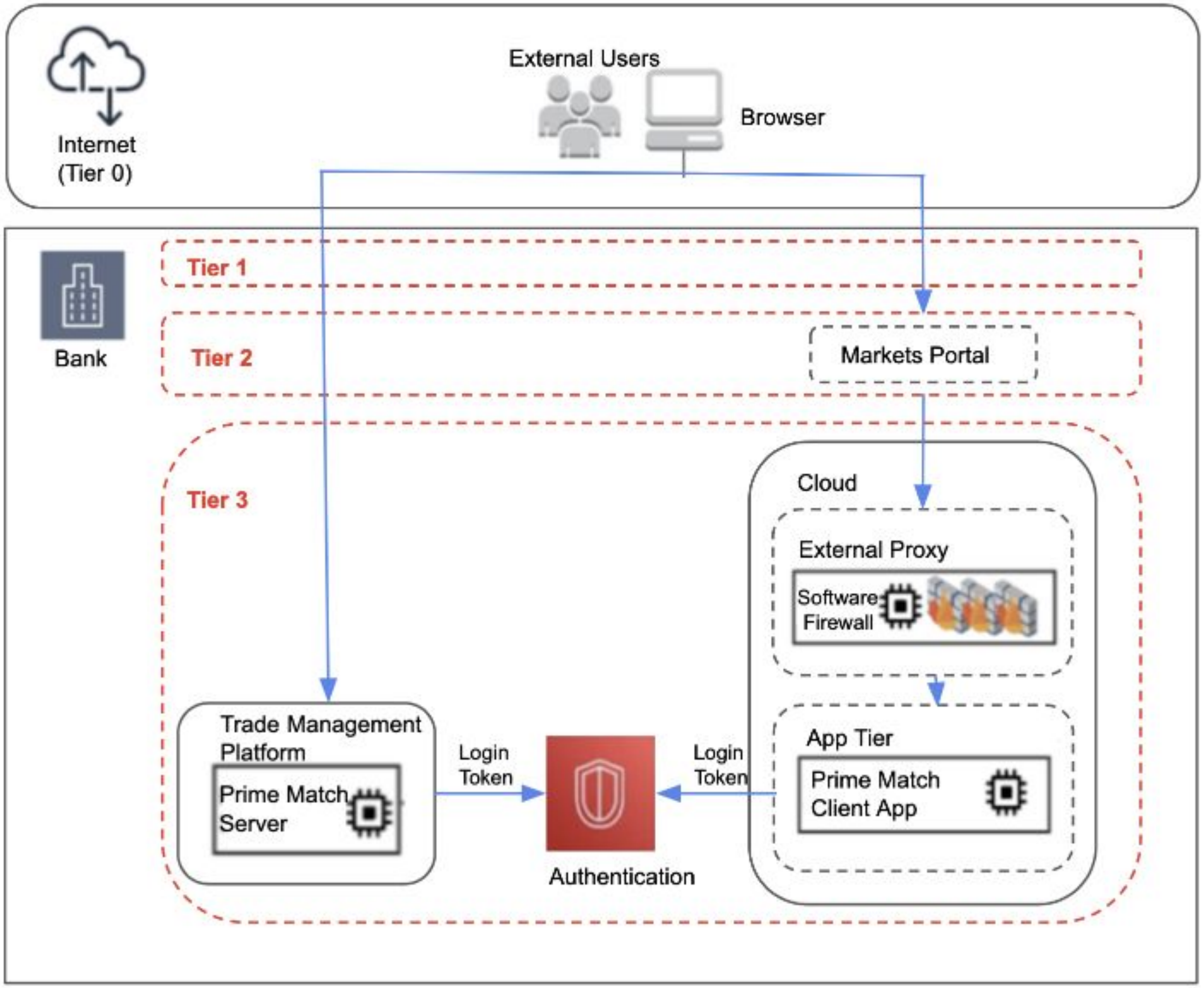
3. Gather comprehensive **client feedback**; requirements and conditions for using Prime Match

**Decided to move in production**

# Prime Match: Client Requirements

- **No communication with other clients**, only communication with the bank
- **No heavy installation of code** on client's machines - a web-based application was required
- Client computation should be **minimal**
- **No resources** for preprocessing data
- **Stronger security guarantees** than semi-honest security
- **Peer review** of the solution
- **Frequent** auctions

# Prime Match: Tech Challenges - Architecture



AlgoCRYPT CoE

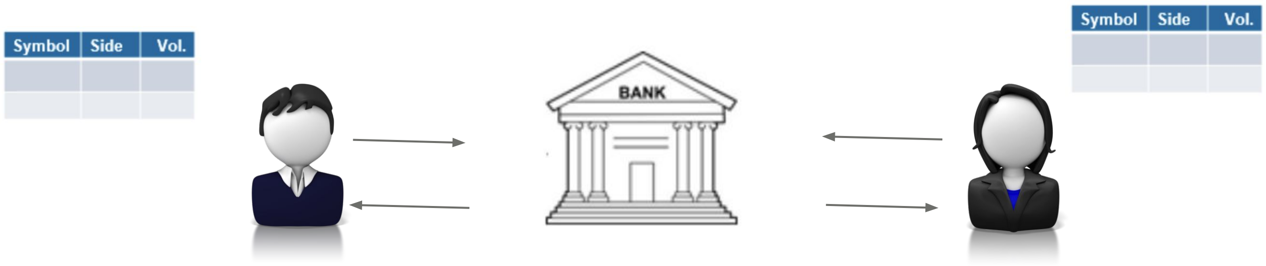
AI Research

J.P.Morgan

# Prime Match: Cryptographic Solution

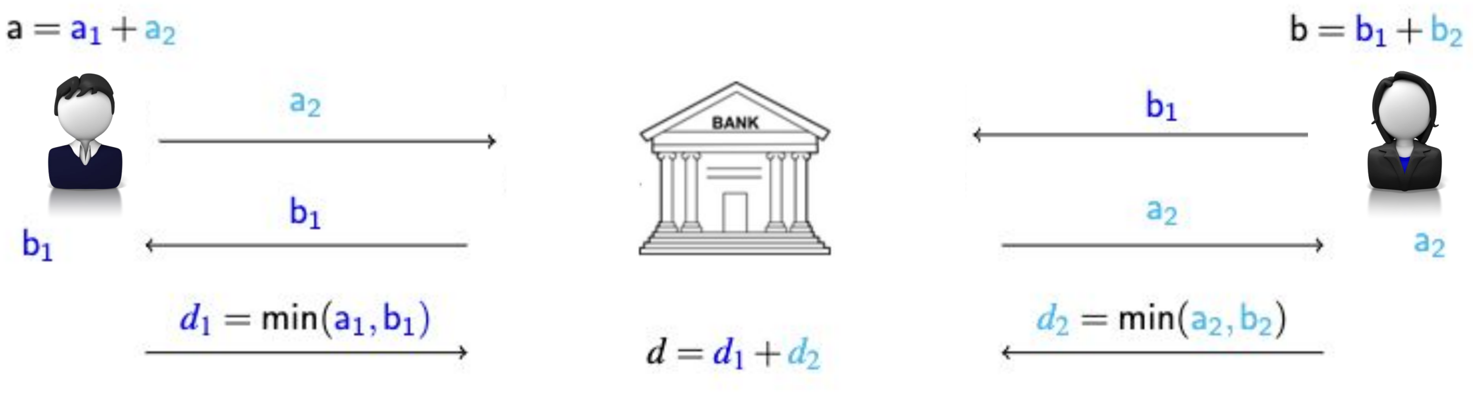
# Cryptographic Contributions in Prime Match

Three-Party Secure comparison with a third party acting as the facilitator:



Three parallel executions

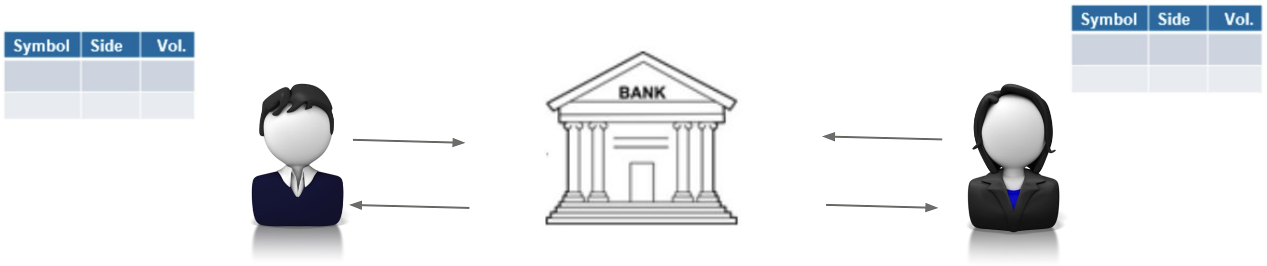
Secret Shared Inputs



New **two-round** secure **linear** comparison protocol

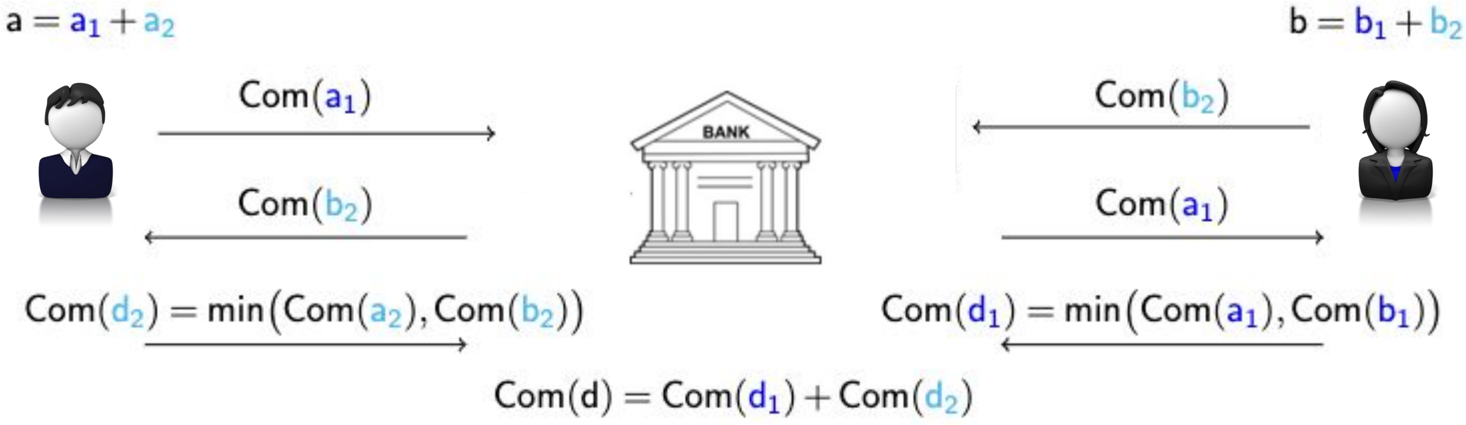
# Cryptographic Contributions in Prime Match

Three-Party Secure comparison with a third party acting as the facilitator:



Three parallel executions

Committed Secret Shares



$a = a_1 + a_2$

$b = b_1 + b_2$

$\mathsf{Com}(a_1)$

$\mathsf{Com}(b_2)$

$\mathsf{Com}(b_2)$

$\mathsf{Com}(a_1)$

$\mathsf{Com}(d_2) = \min(\mathsf{Com}(a_2), \mathsf{Com}(b_2))$

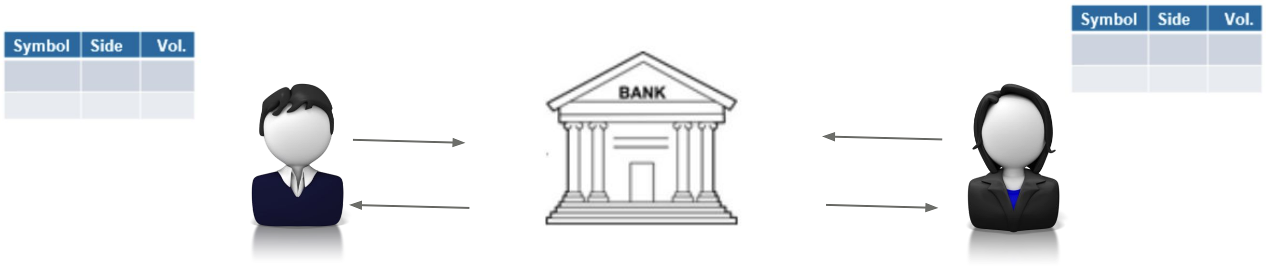
$\mathsf{Com}(d_1) = \min(\mathsf{Com}(a_1), \mathsf{Com}(b_1))$

$\mathsf{Com}(d) = \mathsf{Com}(d_1) + \mathsf{Com}(d_2)$

New **two-round** secure **linear** comparison protocol

# Cryptographic Contributions in Prime Match

## Three-Party Secure comparison with a third party acting as the facilitator:



Registration phase +
Three parallel executions

Openings of Committed Shares

New **two-round** secure **linear** comparison protocol

# Prime Match: High Level Solution

Registration Phase: Need for committed computation

Matching Phase: web based support → low round complexity and communication

Improved version of SecureNN [WaghGuptaChandran19]

**High level of Comparison (min) circuit: (output 1 if any di=0)**

❑ $P_0$, $P_1$ compute shares of:

$$\mathbf{c_i = 1 - a_i + b_i + \Sigma_{j>i}\, r_j\, (a_j - b_j)}$$

❑ $P_0$, $P_1$ send to bank shares of $s_i * c_i$

❑ Bank reconstructs $d_i = s_i * c_i$ and outputs 1 (a>b) if **any** $s_i * c_i = 0$

J.P.Morgan

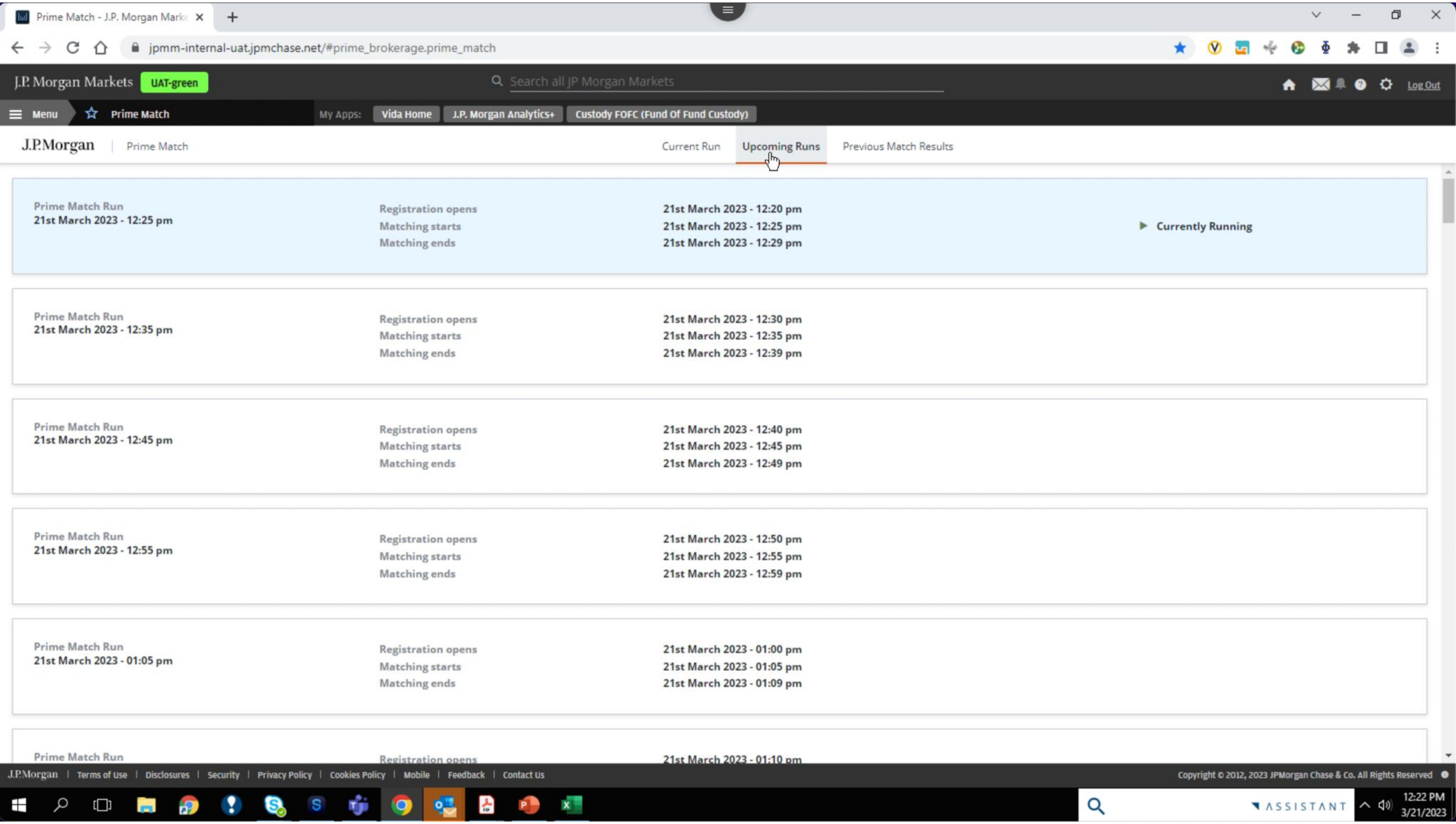
AlgoCRYPT CoE

AI Research

# Prime Match: Tech Challenges - Architecture

Demo

# Prime Match Demo: Auction Runs



Prime Match Run
21st March 2023 - 12:25 pm
Registration opens 21st March 2023 - 12:20 pm
Matching starts 21st March 2023 - 12:25 pm
Matching ends 21st March 2023 - 12:29 pm
▶ Currently Running

Prime Match Run
21st March 2023 - 12:35 pm
Registration opens 21st March 2023 - 12:30 pm
Matching starts 21st March 2023 - 12:35 pm
Matching ends 21st March 2023 - 12:39 pm

Prime Match Run
21st March 2023 - 12:45 pm
Registration opens 21st March 2023 - 12:40 pm
Matching starts 21st March 2023 - 12:45 pm
Matching ends 21st March 2023 - 12:49 pm

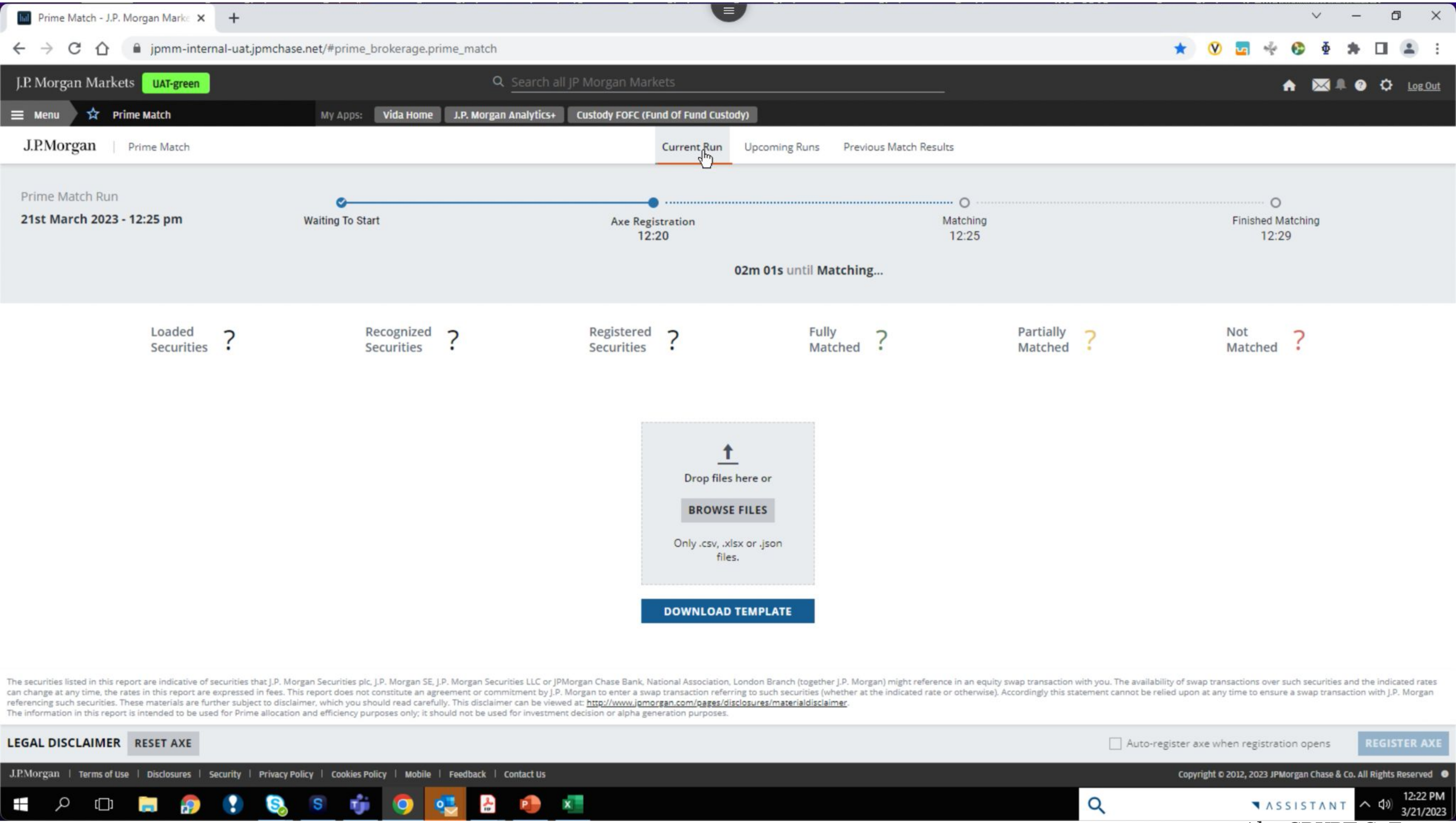
Prime Match Run
21st March 2023 - 12:55 pm
Registration opens 21st March 2023 - 12:50 pm
Matching starts 21st March 2023 - 12:55 pm
Matching ends 21st March 2023 - 12:59 pm

Prime Match Run
21st March 2023 - 01:05 pm
Registration opens 21st March 2023 - 01:00 pm
Matching starts 21st March 2023 - 01:05 pm
Matching ends 21st March 2023 - 01:09 pm

Prime Match Run
Registration opens 21st March 2023 - 01:10 pm

J.P.Morgan | Terms of Use | Disclosures | Security | Privacy Policy | Cookies Policy | Mobile | Feedback | Contact Us
Copyright © 2012, 2023 JPMorgan Chase & Co. All Rights Reserved
ASSISTANT
12:22 PM
3/21/2023

# Prime Match Demo: Registration Phase



Prime Match Run
**21st March 2023 - 12:25 pm**

| Waiting To Start | Axe Registration | Matching | Finished Matching |
|---|---|---|---|
| | 12:20 | 12:25 | 12:29 |

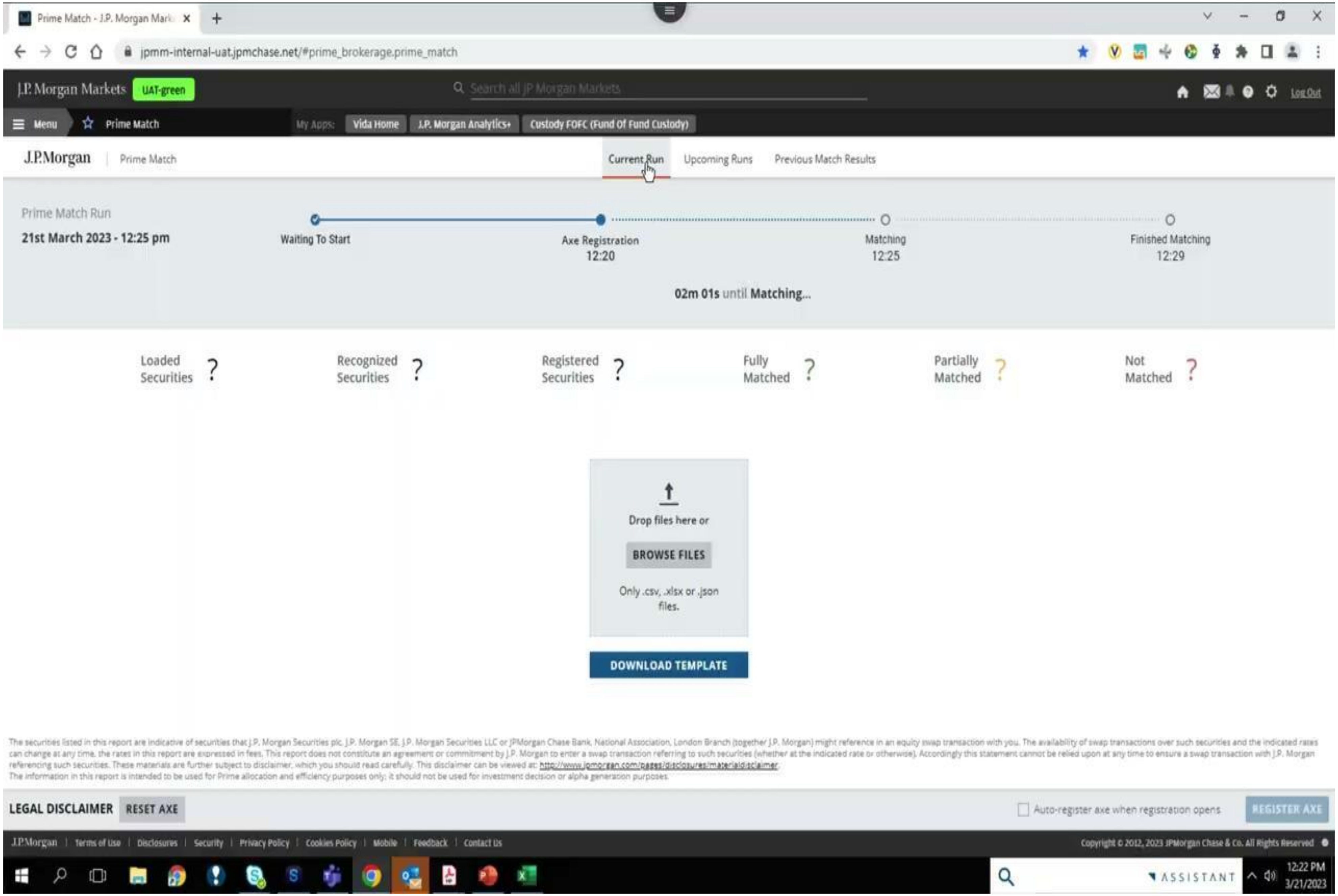
**02m 01s** until **Matching...**

| Loaded Securities | Recognized Securities | Registered Securities | Fully Matched | Partially Matched | Not Matched |
|---|---|---|---|---|---|
| ? | ? | ? | ? | ? | ? |

The securities listed in this report are indicative of securities that J.P. Morgan Securities plc, J.P. Morgan SE, J.P. Morgan Securities LLC or JPMorgan Chase Bank, National Association, London Branch (together J.P. Morgan) might reference in an equity swap transaction with you. The availability of swap transactions over such securities and the indicated rates can change at any time, the rates in this report are expressed in fees. This report does not constitute an agreement or commitment by J.P. Morgan to enter a swap transaction referring to such securities (whether at the indicated rate or otherwise). Accordingly this statement cannot be relied upon at any time to ensure a swap transaction with J.P. Morgan referencing such securities. These materials are further subject to disclaimer, which you should read carefully. This disclaimer can be viewed at: http://www.jpmorgan.com/pages/disclosures/materialdisclaimer.
The information in this report is intended to be used for Prime allocation and efficiency purposes only; it should not be used for investment decision or alpha generation purposes.

LEGAL DISCLAIMER
RESET AXE
□ Auto-register axe when registration opens
REGISTER AXE
J.P.Morgan | Terms of Use | Disclosures | Security | Privacy Policy | Cookies Policy | Mobile | Feedback | Contact Us

# Prime Match Demo: Registration Phase



Prime Match Run

**21st March 2023 - 12:25 pm**

**02m 01s** until **Matching...**

| Loaded Securities | Recognized Securities | Registered Securities | Fully Matched | Partially Matched | Not Matched |
|---|---|---|---|---|---|
| ? | ? | ? | ? | ? | ? |

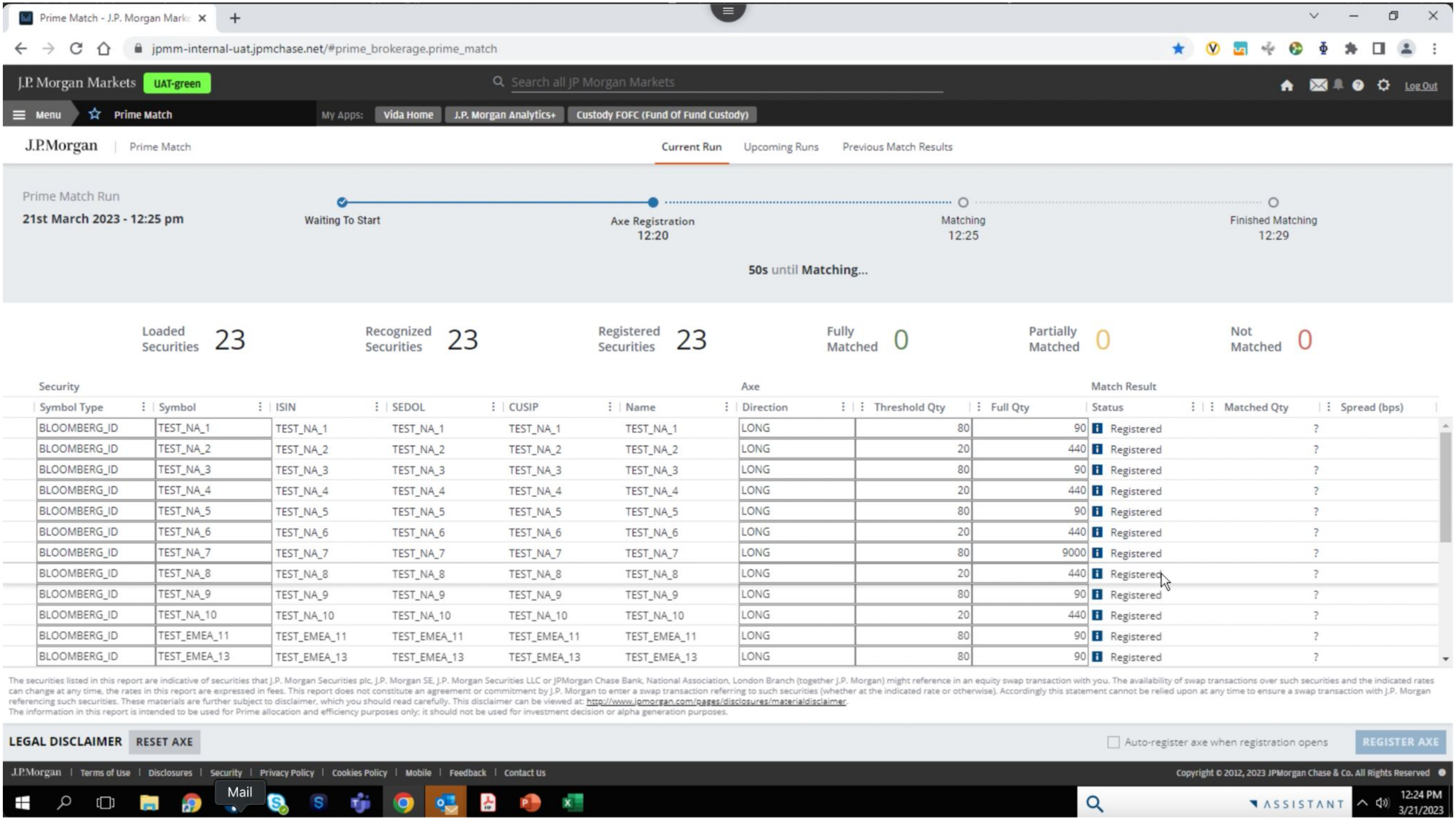
The securities listed in this report are indicative of securities that J.P. Morgan Securities plc, J.P. Morgan SE, J.P. Morgan Securities LLC or JPMorgan Chase Bank, National Association, London Branch (together J.P. Morgan) might reference in an equity swap transaction with you. The availability of swap transactions over such securities and the indicated rates can change at any time. the rates in this report are expressed in fees. This report does not constitute an agreement or commitment by J.P. Morgan to enter a swap transaction referring to such securities (whether at the indicated rate or otherwise). Accordingly this statement cannot be relied upon at any time to ensure a swap transaction with J.P. Morgan referencing such securities. These materials are further subject to disclaimer, which you should read carefully. This disclaimer can be viewed at: http://www.jpmorgan.com/pages/disclosures/materialdisclaimer.
The information in this report is intended to be used for Prime allocation and efficiency purposes only; it should not be used for investment decision or alpha generation purposes.

LEGAL DISCLAIMER
RESET AXE
□ Auto-register axe when registration opens
REGISTER AXE
J.P.Morgan | Terms of Use | Disclosures | Security | Privacy Policy | Cookies Policy | Mobile | Feedback | Contact Us
Copyright © 2012, 2023 JPMorgan Chase & Co. All Rights Reserved
ASSISTANT
12:22 PM
3/21/2023

# Prime Match Demo: Registration Phase

[redacted]

# Prime Match Demo: Registration Phase



Prime Match Run
**21st March 2023 - 12:25 pm**

| Waiting To Start | Axe Registration | Matching | Finished Matching |
|---|---|---|---|
| | 12:20 | 12:25 | 12:29 |

**50s** until **Matching...**

| Loaded Securities | Recognized Securities | Registered Securities | Fully Matched | Partially Matched | Not Matched |
|---|---|---|---|---|---|
| 23 | 23 | 23 | 0 | 0 | 0 |

| Security | | | | | | Axe | | | Match Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Symbol Type | Symbol | ISIN | SEDOL | CUSIP | Name | Direction | Threshold Qty | Full Qty | Status | Matched Qty | Spread (bps) |
| BLOOMBERG_ID | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | LONG | 80 | 90 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | LONG | 20 | 440 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | LONG | 80 | 90 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | LONG | 20 | 440 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | LONG | 80 | 90 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | LONG | 20 | 440 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | LONG | 80 | 9000 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | LONG | 20 | 440 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | LONG | 80 | 90 | Registered | ? | |
| BLOOMBERG_ID | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | LONG | 20 | 440 | Registered | ? | |
| BLOOMBERG_ID | TEST_EMEA_11 | TEST_EMEA_11 | TEST_EMEA_11 | TEST_EMEA_11 | TEST_EMEA_11 | LONG | 80 | 90 | Registered | ? | |
| BLOOMBERG_ID | TEST_EMEA_13 | TEST_EMEA_13 | TEST_EMEA_13 | TEST_EMEA_13 | TEST_EMEA_13 | LONG | 80 | 90 | Registered | ? | |

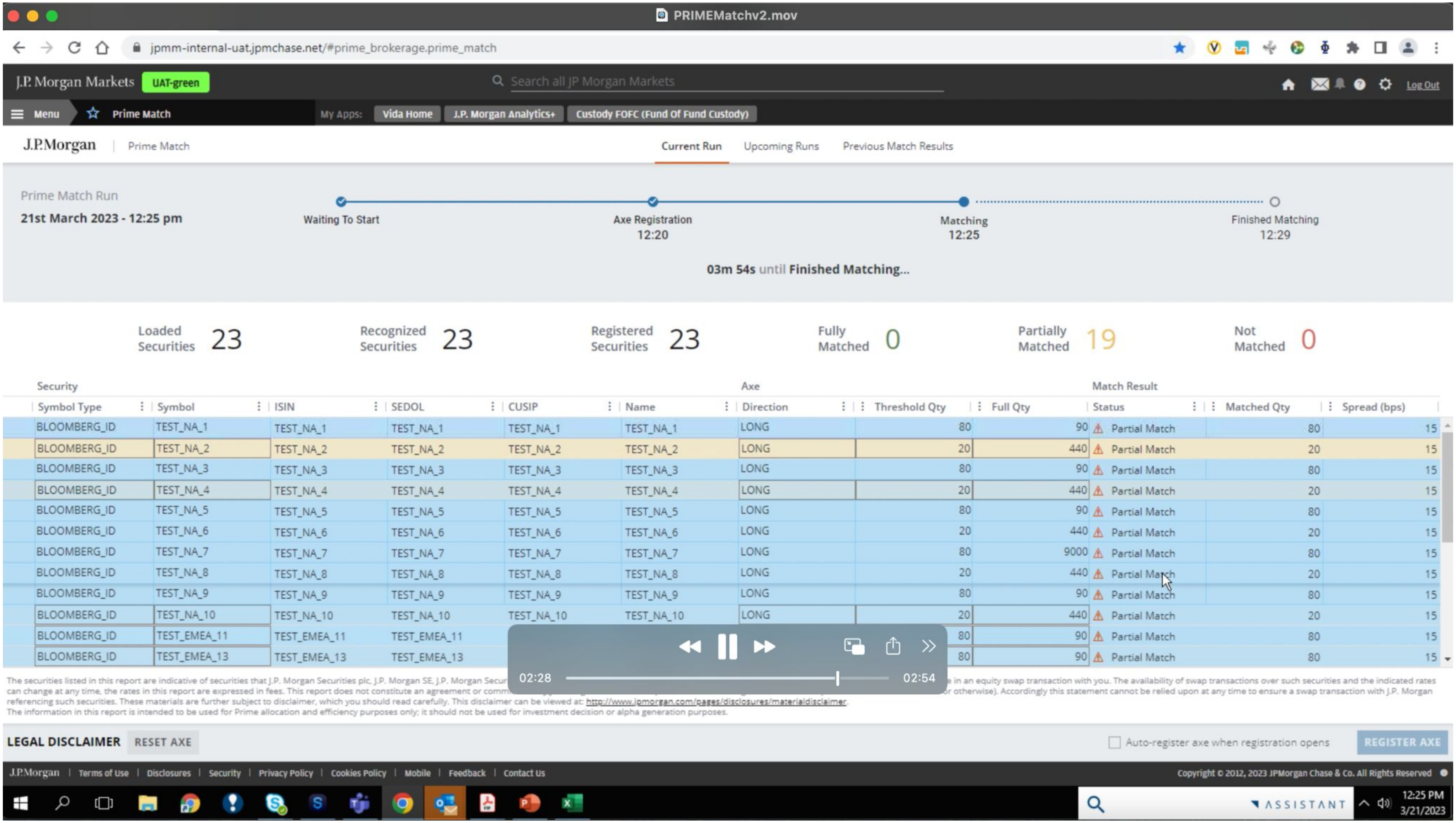
The securities listed in this report are indicative of securities that J.P. Morgan Securities plc, J.P. Morgan SE, J.P. Morgan Securities LLC or JPMorgan Chase Bank, National Association, London Branch (together J.P. Morgan) might reference in an equity swap transaction with you. The availability of swap transactions over such securities and the indicated rates can change at any time, the rates in this report are expressed in fees. This report does not constitute an agreement or commitment by J.P. Morgan to enter a swap transaction referring to such securities (whether at the indicated rate or otherwise). Accordingly this statement cannot be relied upon at any time to ensure a swap transaction with J.P. Morgan referencing such securities. These materials are further subject to disclaimer, which you should read carefully. This disclaimer can be viewed at: http://www.jpmorgan.com/pages/disclosures/materialdisclaimer.
The information in this report is intended to be used for Prime allocation and efficiency purposes only; it should not be used for investment decision or alpha generation purposes.

LEGAL DISCLAIMER
RESET AXE
□ Auto-register axe when registration opens
REGISTER AXE
J.P.Morgan | Terms of Use | Disclosures | Security | Privacy Policy | Cookies Policy | Mobile | Feedback | Contact Us
Mail
ASSISTANT
12:24 PM
3/21/2023

# Prime Match Demo: Matching Phase

# Prime Match Demo: Matching Phase

# Prime Match Demo: Matching Phase



Prime Match Run
**21st March 2023 - 12:25 pm**

**03m 54s** until **Finished Matching...**

| Loaded Securities | Recognized Securities | Registered Securities | Fully Matched | Partially Matched | Not Matched |
|---|---|---|---|---|---|
| 23 | 23 | 23 | 0 | 19 | 0 |

| Security | | | | | | Axe | | | Match Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Symbol Type | Symbol | ISIN | SEDOL | CUSIP | Name | Direction | Threshold Qty | Full Qty | Status | Matched Qty | Spread (bps) |
| BLOOMBERG_ID | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | LONG | 80 | 90 | ⚠ Partial Match | 80 | 15 |
| BLOOMBERG_ID | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | LONG | 20 | 440 | ⚠ Partial Match | 20 | 15 |
| BLOOMBERG_ID | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | LONG | 80 | 90 | ⚠ Partial Match | 80 | 15 |
| BLOOMBERG_ID | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | LONG | 20 | 440 | ⚠ Partial Match | 20 | 15 |
| BLOOMBERG_ID | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | LONG | 80 | 90 | ⚠ Partial Match | 80 | 15 |
| BLOOMBERG_ID | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | LONG | 20 | 440 | ⚠ Partial Match | 20 | 15 |
| BLOOMBERG_ID | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | LONG | 80 | 9000 | ⚠ Partial Match | 80 | 15 |
| BLOOMBERG_ID | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | LONG | 20 | 440 | ⚠ Partial Match | 20 | 15 |
| BLOOMBERG_ID | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | LONG | 80 | 90 | ⚠ Partial Match | 80 | 15 |
| BLOOMBERG_ID | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | LONG | 20 | 440 | ⚠ Partial Match | 20 | 15 |
| BLOOMBERG_ID | TEST_EMEA_11 | TEST_EMEA_11 | TEST_EMEA_11 | | | | 80 | 90 | ⚠ Partial Match | 80 | 15 |
| BLOOMBERG_ID | TEST_EMEA_13 | TEST_EMEA_13 | TEST_EMEA_13 | | | | 80 | 90 | ⚠ Partial Match | 80 | 15 |

The securities listed in this report are indicative of securities that J.P. Morgan Securities plc, J.P. Morgan SE, J.P. Morgan Secur e in an equity swap transaction with you. The availability of swap transactions over such securities and the indicated rates can change at any time, the rates in this report are expressed in fees. This report does not constitute an agreement or comm or otherwise). Accordingly this statement cannot be relied upon at any time to ensure a swap transaction with J.P. Morgan referencing such securities. These materials are further subject to disclaimer, which you should read carefully. This disclaimer can be viewed at: http://www.jpmorgan.com/pages/disclosures/materialdisclaimer.
The information in this report is intended to be used for Prime allocation and efficiency purposes only; it should not be used for investment decision or alpha generation purposes.

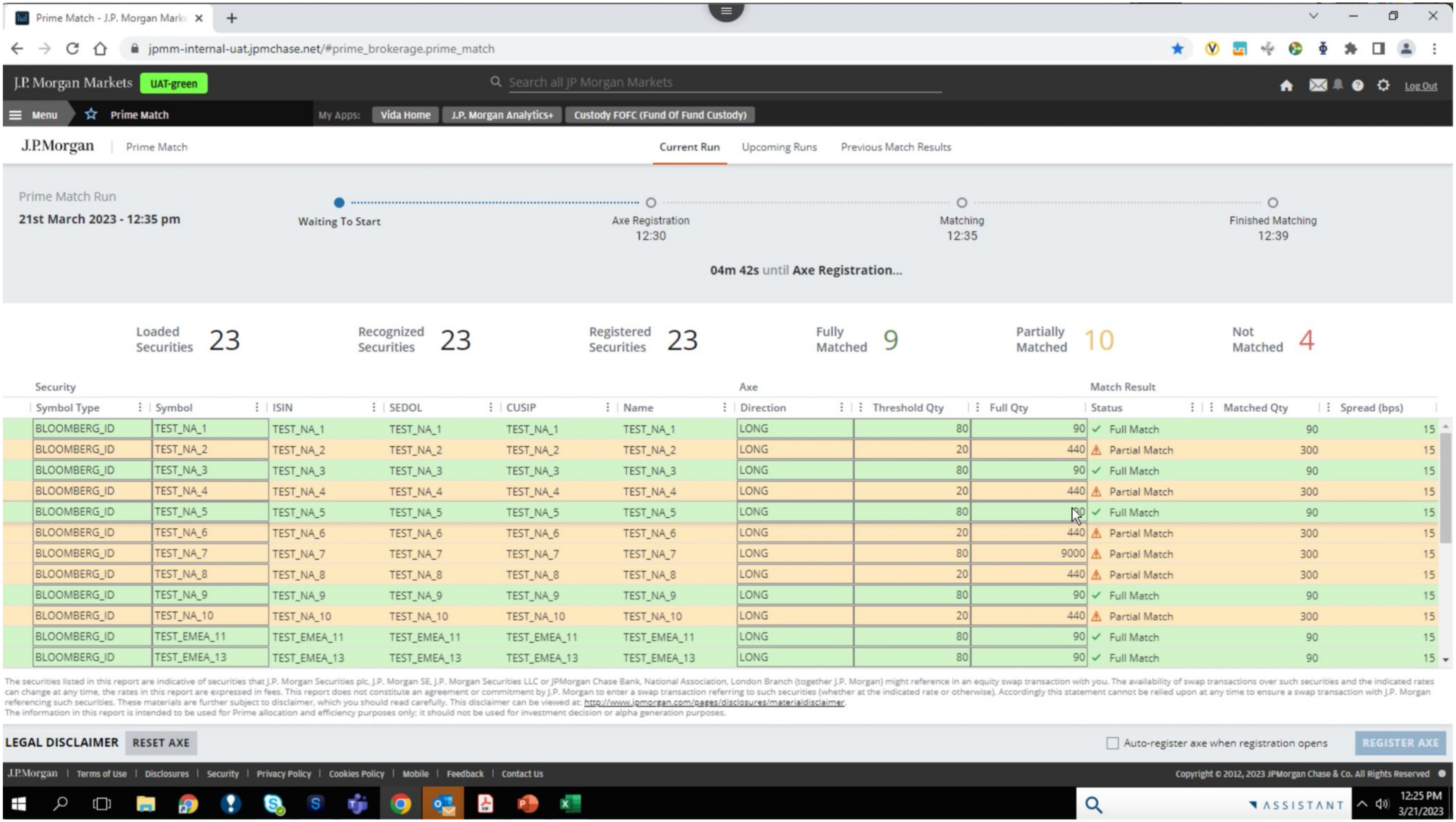
LEGAL DISCLAIMER
RESET AXE
□ Auto-register axe when registration opens
REGISTER AXE
J.P.Morgan | Terms of Use | Disclosures | Security | Privacy Policy | Cookies Policy | Mobile | Feedback | Contact Us
Copyright © 2012, 2023 JPMorgan Chase & Co. All Rights Reserved
ASSISTANT
12:25 PM
3/21/2023

J.P.Morgan

AlgoCRYPT CoE

AI Research

# Prime Match Demo: Matching Phase


Prime Match - J.P. Morgan Marke ×
jpmm-internal-uat.jpmchase.net/#prime_brokerage.prime_match
J.P. Morgan Markets UAT-green
Search all JP Morgan Markets
Log Out
Menu
Prime Match
My Apps: Vida Home J.P. Morgan Analytics+ Custody FOFC (Fund Of Fund Custody)
J.P.Morgan | Prime Match
Current Run
Upcoming Runs
Previous Match Results

Prime Match Run
**21st March 2023 - 12:35 pm**

Waiting To Start — Axe Registration 12:30 — Matching 12:35 — Finished Matching 12:39

**04m 42s** until **Axe Registration...**

| Loaded Securities | Recognized Securities | Registered Securities | Fully Matched | Partially Matched | Not Matched |
|---|---|---|---|---|---|
| 23 | 23 | 23 | 9 | 10 | 4 |

| Security | | | | | | Axe | | | Match Result | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Symbol Type | Symbol | ISIN | SEDOL | CUSIP | Name | Direction | Threshold Qty | Full Qty | Status | Matched Qty | Spread (bps) |
| BLOOMBERG_ID | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | TEST_NA_1 | LONG | 80 | 90 | ✓ Full Match | 90 | 15 |
| BLOOMBERG_ID | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | TEST_NA_2 | LONG | 20 | 440 | ⚠ Partial Match | 300 | 15 |
| BLOOMBERG_ID | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | TEST_NA_3 | LONG | 80 | 90 | ✓ Full Match | 90 | 15 |
| BLOOMBERG_ID | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | TEST_NA_4 | LONG | 20 | 440 | ⚠ Partial Match | 300 | 15 |
| BLOOMBERG_ID | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | TEST_NA_5 | LONG | 80 | 90 | ✓ Full Match | 90 | 15 |
| BLOOMBERG_ID | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | TEST_NA_6 | LONG | 20 | 440 | ⚠ Partial Match | 300 | 15 |
| BLOOMBERG_ID | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | TEST_NA_7 | LONG | 80 | 9000 | ⚠ Partial Match | 300 | 15 |
| BLOOMBERG_ID | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | TEST_NA_8 | LONG | 20 | 440 | ⚠ Partial Match | 300 | 15 |
| BLOOMBERG_ID | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | TEST_NA_9 | LONG | 80 | 90 | ✓ Full Match | 90 | 15 |
| BLOOMBERG_ID | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | TEST_NA_10 | LONG | 20 | 440 | ⚠ Partial Match | 300 | 15 |
| BLOOMBERG_ID | TEST_EMEA_11 | TEST_EMEA_11 | TEST_EMEA_11 | TEST_EMEA_11 | TEST_EMEA_11 | LONG | 80 | 90 | ✓ Full Match | 90 | 15 |
| BLOOMBERG_ID | TEST_EMEA_13 | TEST_EMEA_13 | TEST_EMEA_13 | TEST_EMEA_13 | TEST_EMEA_13 | LONG | 80 | 90 | ✓ Full Match | 90 | 15 |

The securities listed in this report are indicative of securities that J.P. Morgan Securities plc, J.P. Morgan SE, J.P. Morgan Securities LLC or JPMorgan Chase Bank, National Association, London Branch (together J.P. Morgan) might reference in an equity swap transaction with you. The availability of swap transactions over such securities and the indicated rates can change at any time, the rates in this report are expressed in fees. This report does not constitute an agreement or commitment by J.P. Morgan to enter a swap transaction referring to such securities (whether at the indicated rate or otherwise). Accordingly this statement cannot be relied upon at any time to ensure a swap transaction with J.P. Morgan referencing such securities. These materials are further subject to disclaimer, which you should read carefully. This disclaimer can be viewed at: http://www.jpmorgan.com/pages/disclosures/materialdisclaimer.
The information in this report is intended to be used for Prime allocation and efficiency purposes only; it should not be used for investment decision or alpha generation purposes.

LEGAL DISCLAIMER
RESET AXE
□ Auto-register axe when registration opens
REGISTER AXE
J.P.Morgan | Terms of Use | Disclosures | Security | Privacy Policy | Cookies Policy | Mobile | Feedback | Contact Us
Copyright © 2012, 2023 JPMorgan Chase & Co. All Rights Reserved
ASSISTANT
12:25 PM
3/21/2023

AlgoCRYPT CoE

AI Research

# Conclusion

- **Identified a real-world problem for MPC** in which the privacy of the previous inventory matching procedure can be significantly enhanced
- Prime Match protocols—bank-to-client inventory matching and client-to-client inventory matching—completely replace the current method which not only leaks information but also fails to identify potential matches
  - **Our protocols are novel and customized** to the particular use case being addressed (privacy preserving auctions)
- At the core of our matching engine lies a new **two-round comparison** protocol that minimizes interaction and requires **only linear operations**.
- Prime Match protocols are implemented and **run live for the first time, in production**, by a major bank in the US – J.P. Morgan.

# Conclusion and Future Work

Future work:

1. **Fair matching t**hat ensures no single client can monopolize the majority of the inventory.
2. Extend MPC for:
   1. Privacy preserving **darkpools**
   2. Privacy preserving **portfolio optimization**

# Prime Match: A Privacy Preserving Inventory Matching System

ARTIFACT EVALUATED
usenix ASSOCIATION
FUNCTIONAL

ARTIFACT EVALUATED
usenix ASSOCIATION
REPRODUCED

**USENIX Security 2023**

Thank you!

https://eprint.iacr.org/2023/400

RWC 2023 video:

antigoni.polychroniadou@jpmorgan.com
antigonipoly@gmail.com