Fraud Information Sharing Issues and Progress

US Faster Payments Council

SPRING MEMBER MEETING 2024

MARCH 27-28, 2024
LAKE BUENA VISTA, FL

Liam Cooney
Vice President,
Mastercard

Andrew Gomez
Director,
Lipis Advisors

Kalpa Gupta
CEO,
Knekxt Group

Marc Trepanier
Sr Principal Fraud
Consultant,
ACI Worldwide

What is Fraud Information Sharing?

Sharing of intelligence to reduce fraud risks and increase overall trust in payments

The work group will begin exploring information sharing approaches related to scam activity, with a focus on fostering collaboration among the industry to bring about voluntary and collective change in the fight against scams. Work group recommendations for approaches to information sharing are likely to include specific use cases, data types, methods and the benefits of sharing information.

"Fraudsters are using similar tactics across organizations to conduct scams, and lack of information sharing helps fraudsters successfully repeat the same tactics. Timely access to fraud information can help improve fraud management strategies, detect scams more quickly and avoid potentially devastating losses within an organization, as well as within the industry as a whole."

Mike Timoney, vice president of payments improvement

Federal Reserve Financial Services

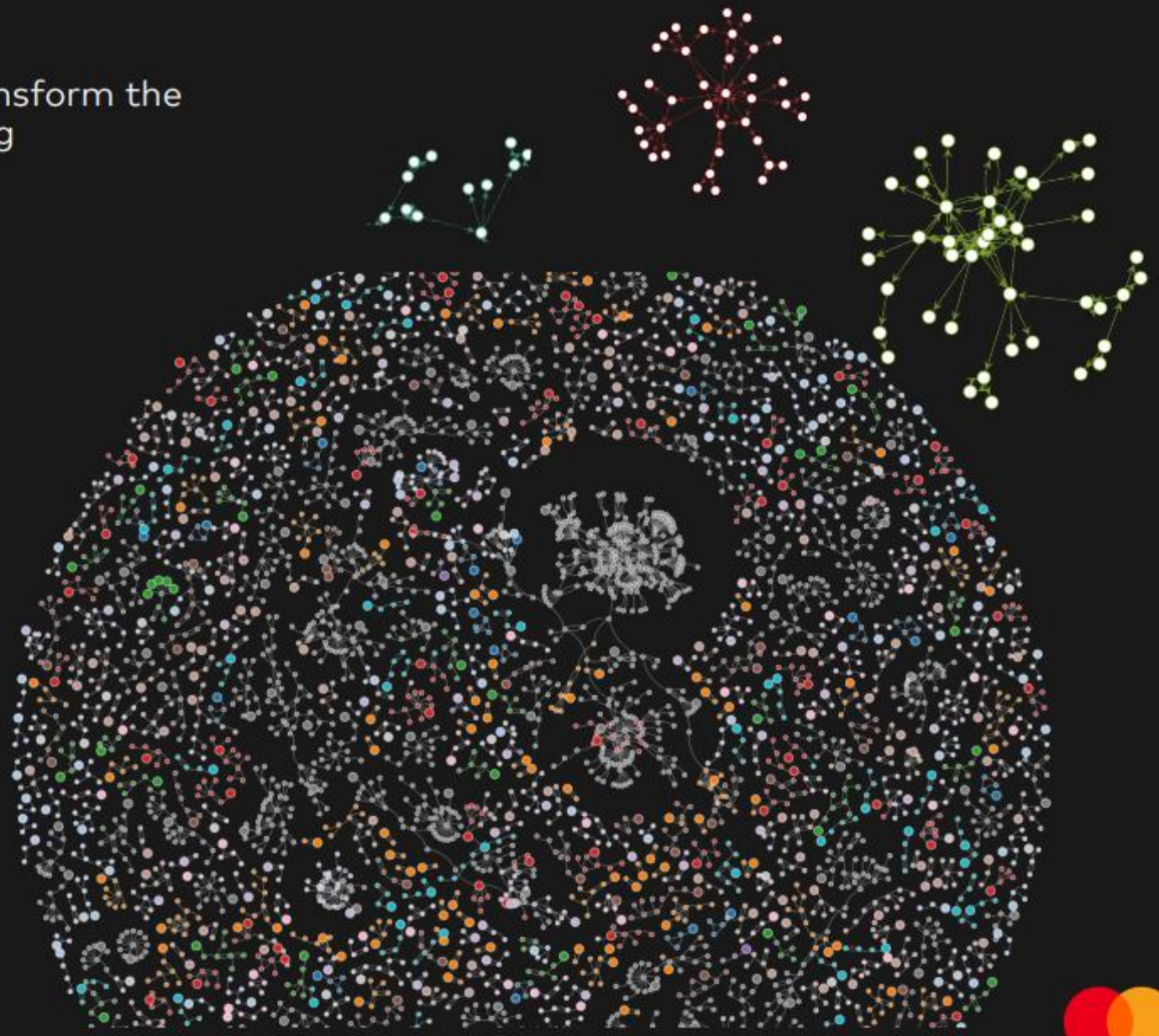
Collaborating in the fight against financial crime

Data used in the right way has the power to transform the fight against scams, fraud and money laundering

Mastercard has spent years focusing and specialising in developing solutions that leverage multi-bank transaction data and insights to **mitigate against Scams, Fraud and Money Laundering**

We've built and developed solutions using **billions of real time and batch payment transactions**, as well as millions of fraud and ML data point each year from numerous countries around the world.

Collaboration across multiple banks in a country is key to provide more accurate scam, fraud and money mule scores that identify good and illicit transactions to enhance individual bank models with additional data points and insights



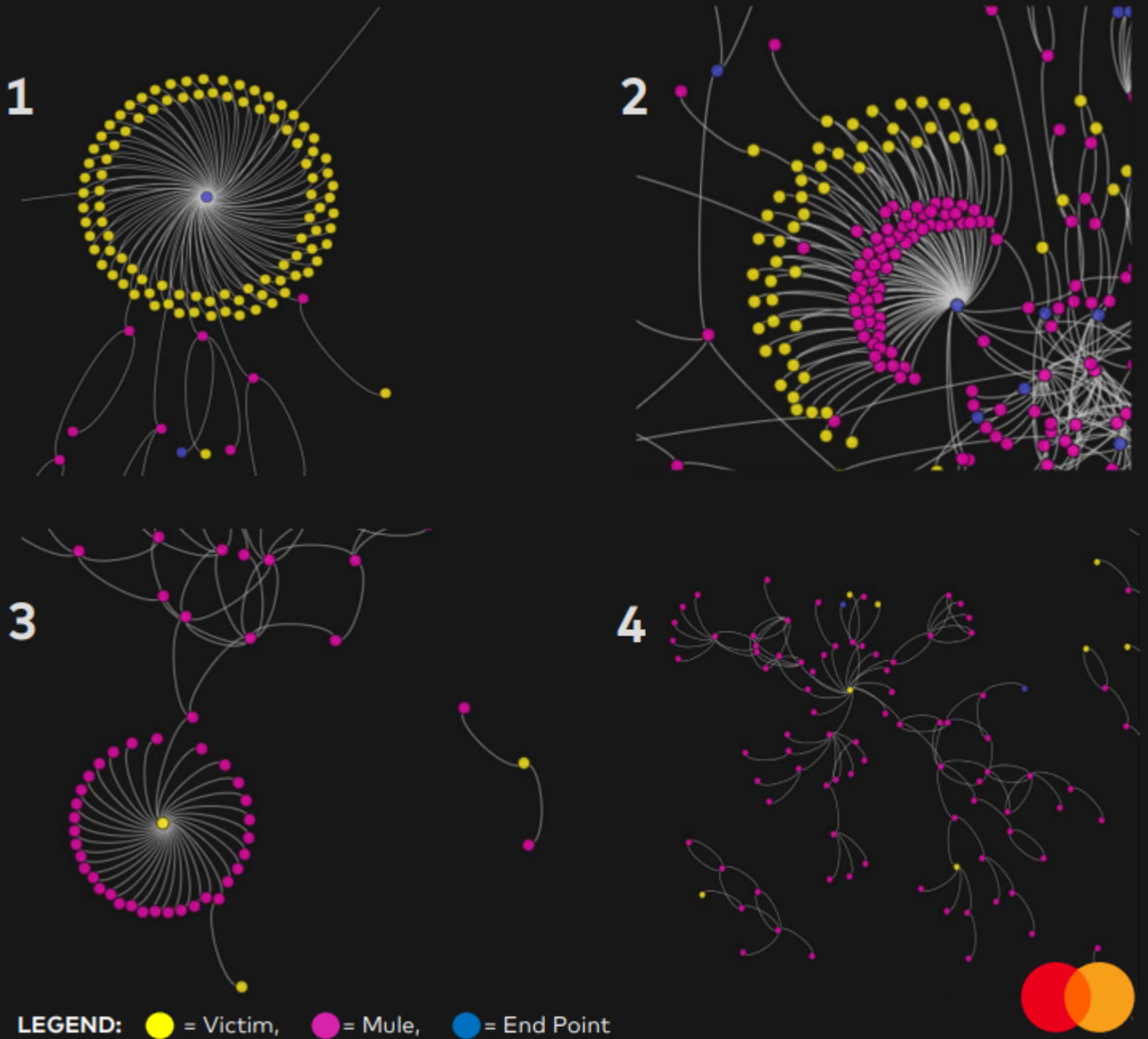
Mult-bank transaction data can unveil hidden fraud, scams and mules

1. Victims of a fraud or scam with one egress point, likely phishing

2. Typical flow from victims to multiple mules to one egress point

3. One victim connected to multiple mule accounts – Likely to be ATO

4. Broader dispersion tree showing flow of laundering



No bank is an island… any fraud diminishes community trust

Two main types of centralized anti-fraud measures: tech-based & rule-based approaches

Techniques		Function								
Technology-based approach	Confirmation-of-Payee(COP)	Allow the payer to confirm the payee's details				✓		✓	✓	
	Fraud monitoring system	Provide a centralized fraud prevention system	✓	✓	✓			✓	✓	
	Fraudulent individual database	Create a database for sharing fraud-related data between multiple parties	✓		✓	✓	✓	✓	✓	
	Cross-industry collaboration	Collaborate with other industries (e.g., telcos) to mitigate certain fraud types (SIM swap, mobile payment fraud)						✓	✓	
	Digital ID system	Use personal identity to strengthen authentication process						✓		
Rule-based approach	Transaction value limits	Set value limits for for certain transaction types or during certain time windows	✓	✓		✓	✓	✓	✓	✓
	Limits on number of transactions per day	Set daily limits on the number of payments		✓						
	Transaction hold for analysis	Set rules that enable participants to conduct more detailed fraud analysis on transactions	✓		✓		✓	✓		✓
	Awareness campaigns aimed at the general public	Create awareness campaigns to spread anti-fraud message to the public			✓	✓		✓	✓	
	Regulatory sandbox	Promote new fraud prevention solutions through a regulatory sandbox focused on fraud prevention ideas	✓	✓	✓	✓	✓	✓	✓	
	Dispute resolution/ loss recovery	Regulations in place regarding fraud resolution/loss recovery for consumer protection purposes	✓	✓		✓				
	Data and QR-code security standards	Create common standards for QR codes with payment security features	✓	✓	✓	✓	✓	✓	✓	
	Enhanced authentication measures	Implement strong customer authentication (e.g., two factor authentication) for account access								

Questions?

Thank you!