Zelle® InfoExchange on Risk Management

Kannan Srinivasan, Vice President, Risk Assurance
Digital Payment Solutions, Fiserv

April 28th 2022

Zelle® InfoExchange

The *Zelle* InfoExchange: An interactive forum designed for Fiserv clients to share risk management-related ideas, challenges and opportunities with other *Zelle* participants and the Fiserv team.

Risk mitigation focus

Client experience, fraud operations and more

A Strong Focus on You – Our Client

Agenda

- EWS / Zelle Monthly Fraud Update
- Fiserv Zelle Turnkey Frauds

Zelle®

Zelle ® Fraud Risk – Monthly Touch Base

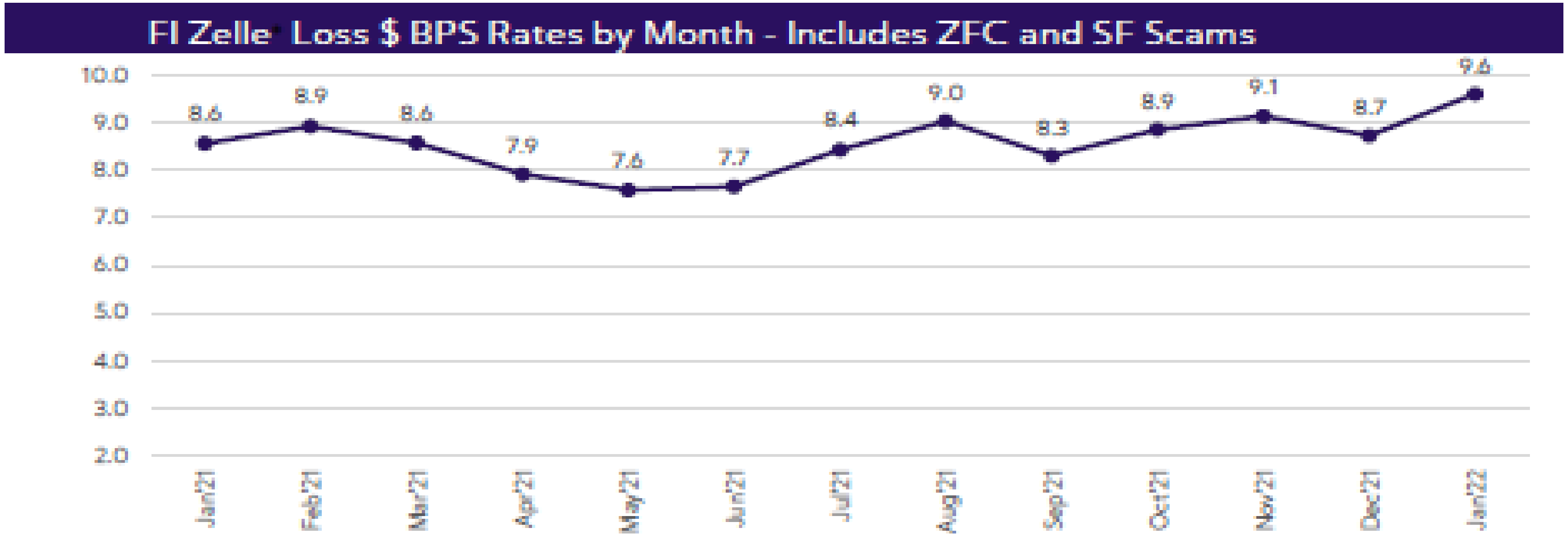
March 24, 2022

Notice

- This document contains confidential and proprietary information of Early Warning Services, LLC ("Early Warning"). It must not be used, duplicated, distributed or disclosed, in whole or in part, except in accordance with the terms of a valid confidentiality agreement between Early Warning and your employer or with prior written consent from Early Warning.

Fraud Metrics

Zelle® Reported Fraud – In Network View by Transaction Month

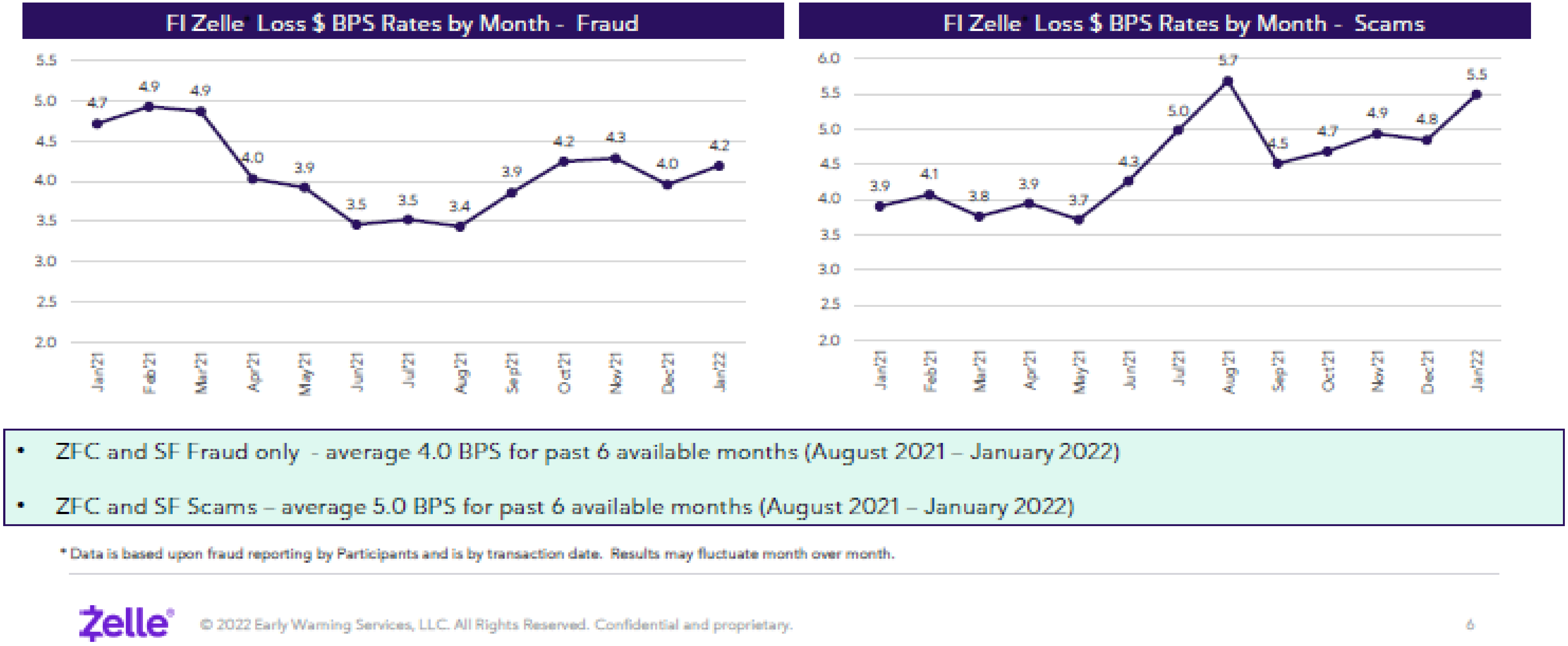


FI Zelle® Loss $ BPS Rates by Month - Includes ZFC and SF Scams

- ZFC and SF Fraud - average 9.0 BPS for past 6 available months (August 2021 – January 2022)

* Data is based upon fraud reporting by Participants and is by transaction date. Results may fluctuate month over month.

Zelle® Reported Fraud – In Network View by Transaction Month


FI Zelle* Loss $ BPS Rates by Month - Fraud

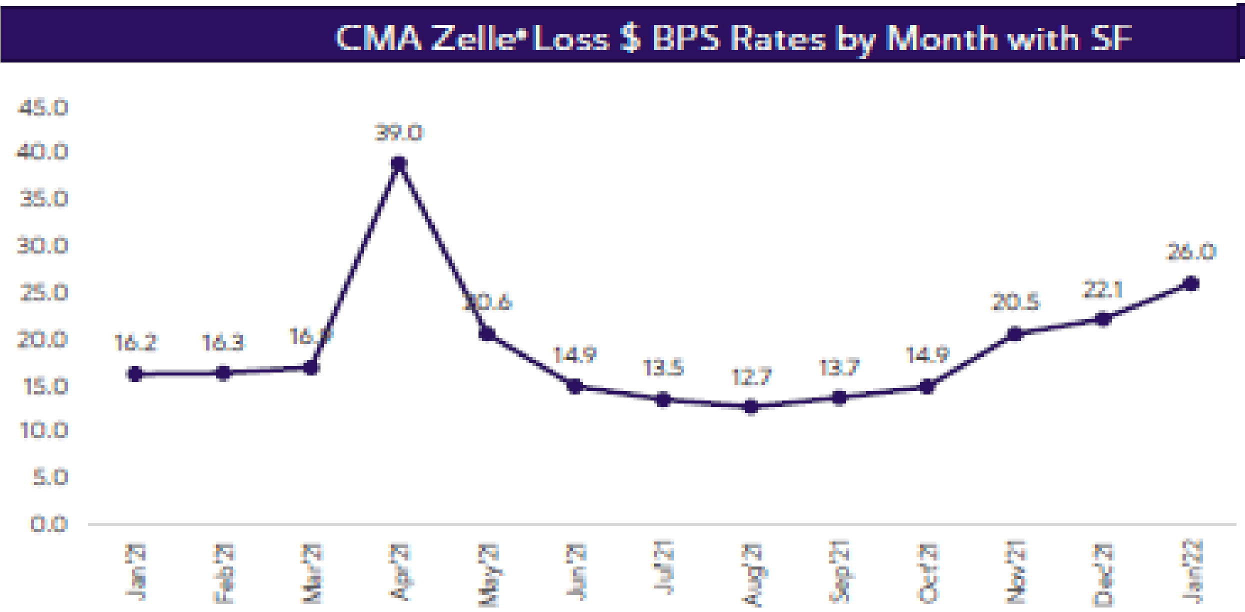
FI Zelle* Loss $ BPS Rates by Month - Scams

- ZFC and SF Fraud only - average 4.0 BPS for past 6 available months (August 2021 – January 2022)
- ZFC and SF Scams – average 5.0 BPS for past 6 available months (August 2021 – January 2022)

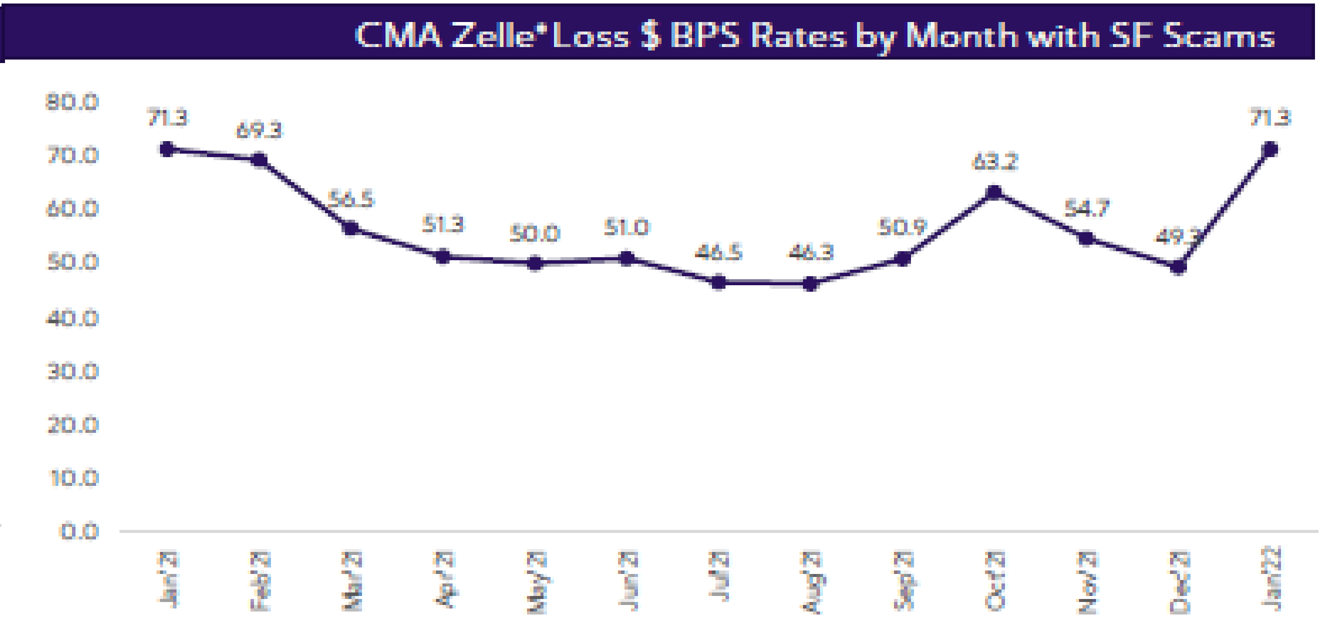
* Data is based upon fraud reporting by Participants and is by transaction date. Results may fluctuate month over month.

Zelle® Reported Fraud – Common Mobile App by Transaction Month

Send

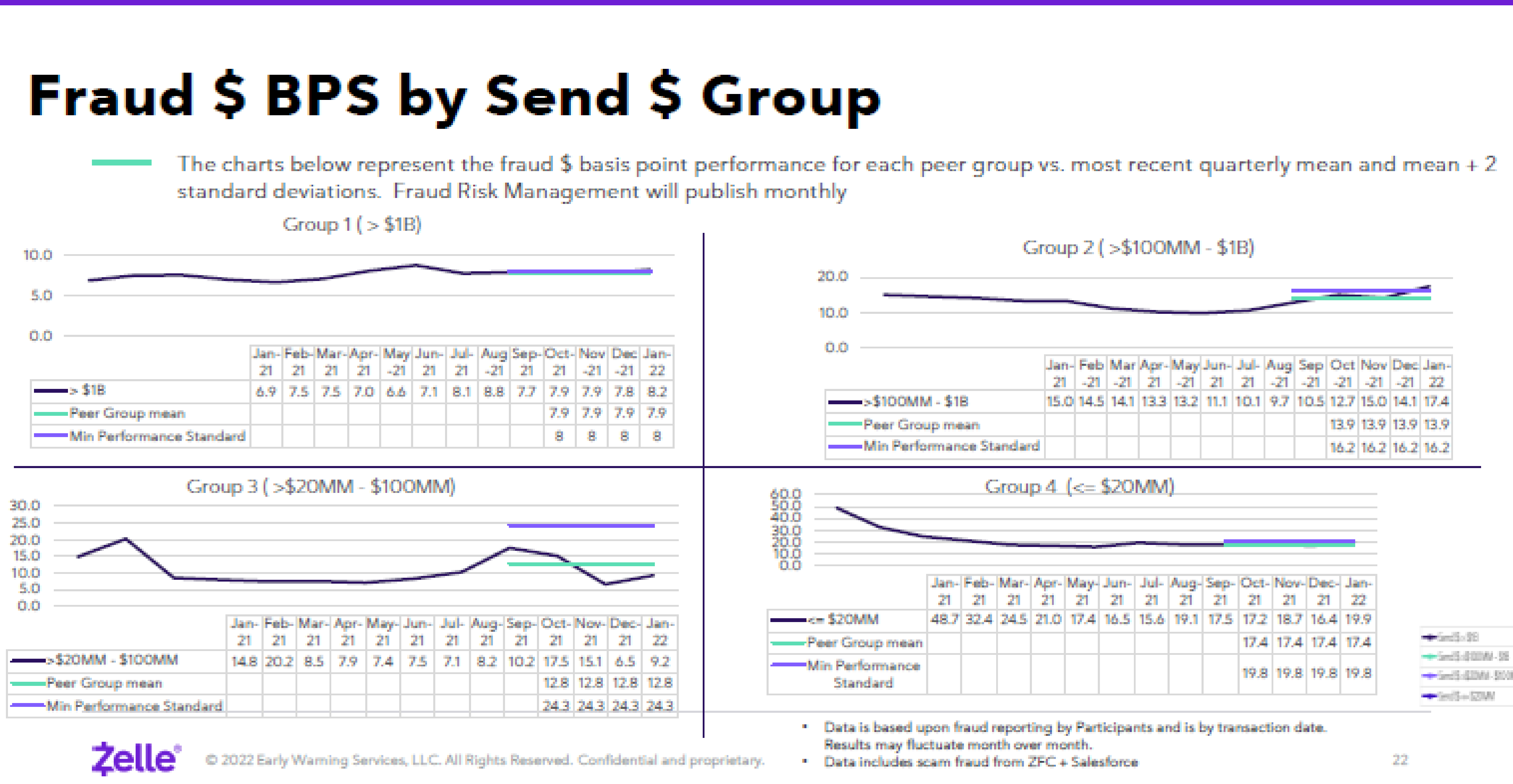

CMA Zelle® Loss $ BPS Rates by Month with SF

Receive


CMA Zelle® Loss $ BPS Rates by Month with SF Scams

- Average Sending Fraud BPs for past 6 months (August 2021 – January 2022) is **18.3 BPs**
- Average Receiving Fraud BPs for last 6 months (August 2021 – January 2022) is **56 BPs**
- CMA send and receive fraud driven by:
  - Fraud rings in Alabama & Mississippi.
  - Fraud from banks with lesser Know Your Customers (KYC) requirements.
  - Fraud from older mobile devices using T-Mobile.
  - Newer emails used to register.
  - Missing connection data / users electing to not share location at enrollment.
- Countermeasures: rules and strategies targeting fraud rings, risky regions, older mobile phones and missing connection data (~53% of send and receive Feb fraud/scam to be mitigated).

* Data is based upon fraud reporting by Participants and is by transaction date. Results may fluctuate month over month.



Fraud $ BPS by Send $ Group

The charts below represent the fraud $ basis point performance for each peer group vs. most recent quarterly mean and mean + 2 standard deviations. Fraud Risk Management will publish monthly

Group 1 (> $1B)

	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22
> $1B	6.9	7.5	7.5	7.0	6.6	7.1	8.1	8.8	7.7	7.9	7.9	7.8	8.2
Peer Group mean										7.9	7.9	7.9	7.9
Min Performance Standard										8	8	8	8

Group 2 (>$100MM - $1B)

	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22
>$100MM - $1B	15.0	14.5	14.1	13.3	13.2	11.1	10.1	9.7	10.5	12.7	15.0	14.1	17.4
Peer Group mean										13.9	13.9	13.9	13.9
Min Performance Standard										16.2	16.2	16.2	16.2

Group 3 (>$20MM - $100MM)

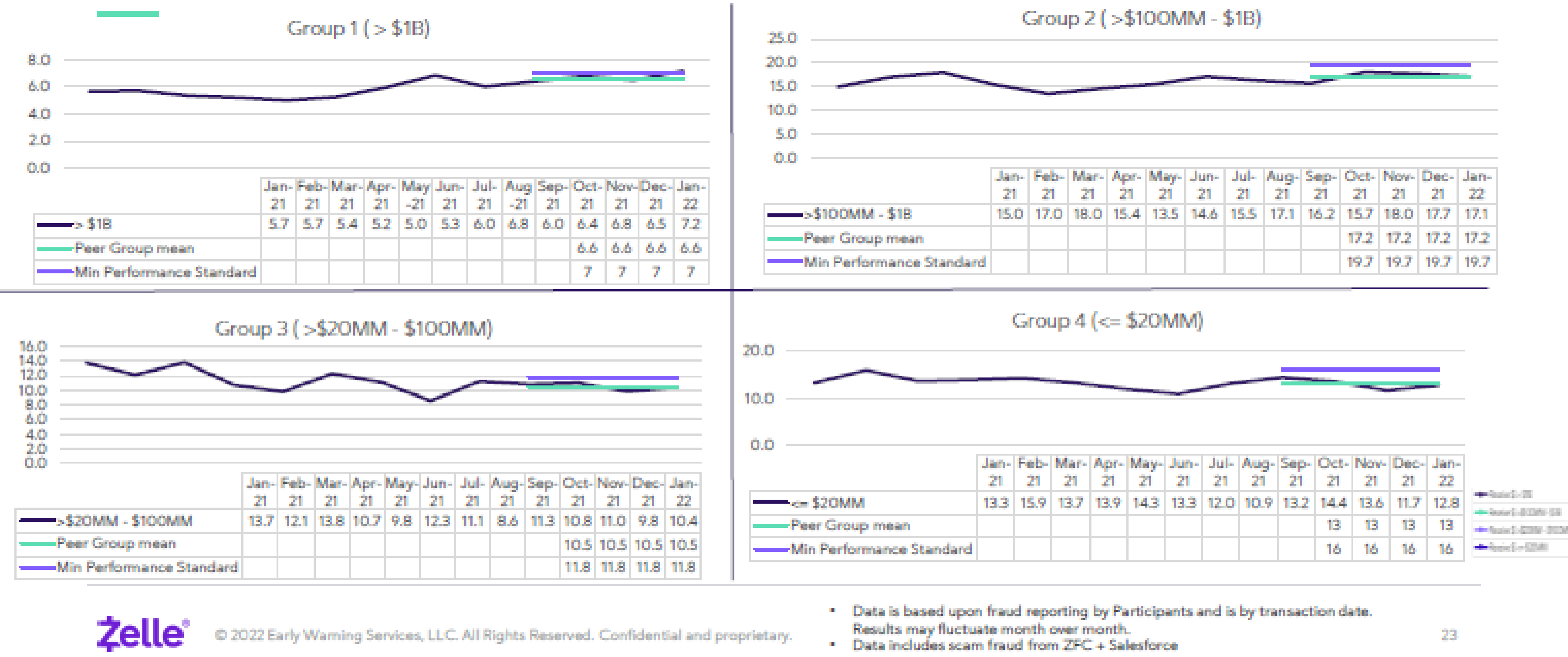
	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22
>$20MM - $100MM	14.8	20.2	8.5	7.9	7.4	7.5	7.1	8.2	10.2	17.5	15.1	6.5	9.2
Peer Group mean										12.8	12.8	12.8	12.8
Min Performance Standard										24.3	24.3	24.3	24.3

Group 4 (<= $20MM)

	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22
<= $20MM	48.7	32.4	24.5	21.0	17.4	16.5	15.6	19.1	17.5	17.2	18.7	16.4	19.9
Peer Group mean										17.4	17.4	17.4	17.4
Min Performance Standard										19.8	19.8	19.8	19.8

- Data is based upon fraud reporting by Participants and is by transaction date. Results may fluctuate month over month.
- Data includes scam fraud from ZFC + Salesforce

Fraud $ BPS by Receive $ Group



Group 1 (> $1B)

	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22
> $1B	5.7	5.7	5.4	5.2	5.0	5.3	6.0	6.8	6.0	6.4	6.8	6.5	7.2
Peer Group mean										6.6	6.6	6.6	6.6
Min Performance Standard										7	7	7	7

Group 2 (>$100MM - $1B)

	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22
>$100MM - $1B	15.0	17.0	18.0	15.4	13.5	14.6	15.5	17.1	16.2	15.7	18.0	17.7	17.1
Peer Group mean										17.2	17.2	17.2	17.2
Min Performance Standard										19.7	19.7	19.7	19.7

Group 3 (>$20MM - $100MM)

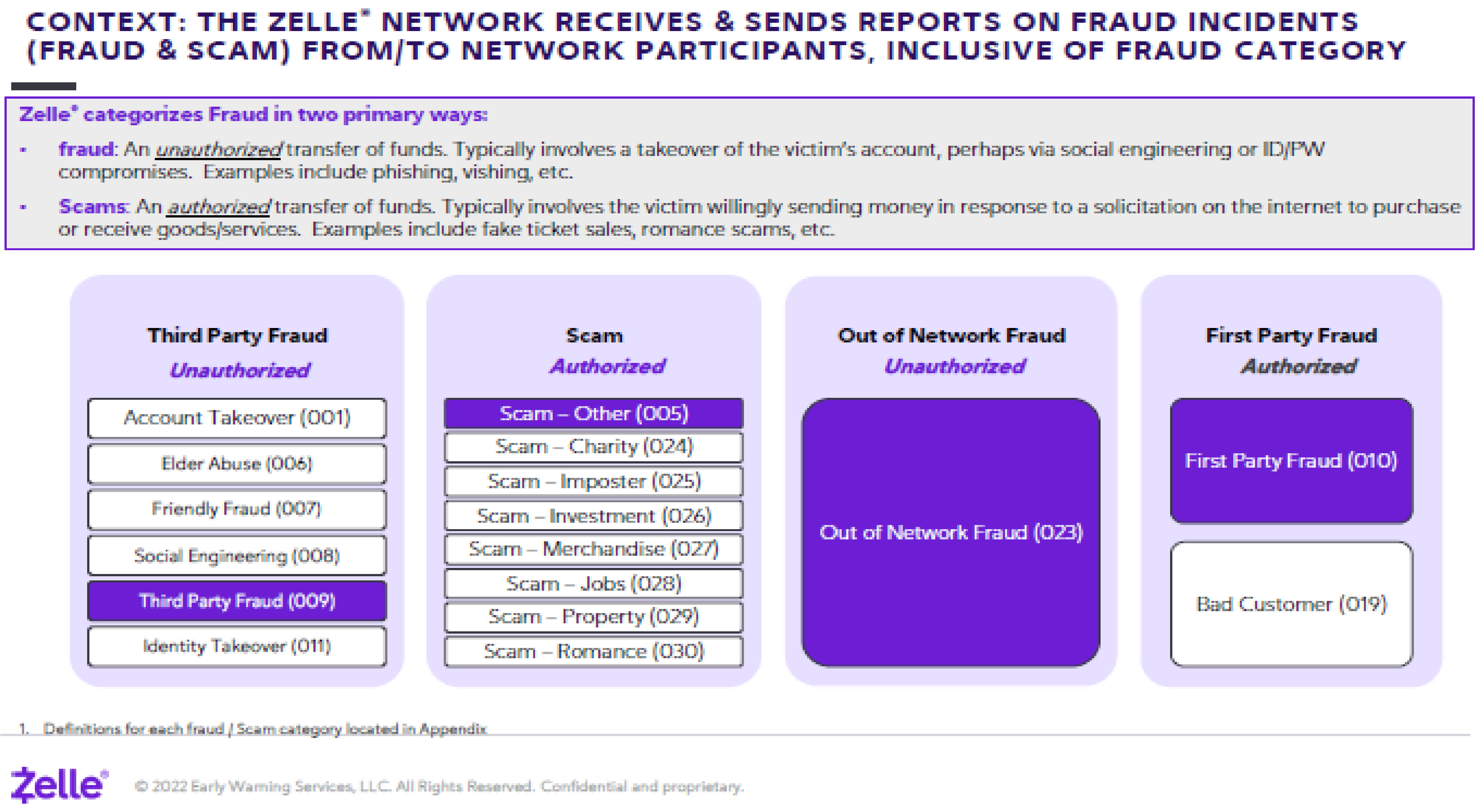
	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22
>$20MM - $100MM	13.7	12.1	13.8	10.7	9.8	12.3	11.1	8.6	11.3	10.8	11.0	9.8	10.4
Peer Group mean										10.5	10.5	10.5	10.5
Min Performance Standard										11.8	11.8	11.8	11.8

Group 4 (<= $20MM)

	Jan-21	Feb-21	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22
<= $20MM	13.3	15.9	13.7	13.9	14.3	13.3	12.0	10.9	13.2	14.4	13.6	11.7	12.8
Peer Group mean										13	13	13	13
Min Performance Standard										16	16	16	16

Zelle

- Data is based upon fraud reporting by Participants and is by transaction date. Results may fluctuate month over month.
- Data includes scam fraud from ZFC + Salesforce



CONTEXT: THE ZELLE® NETWORK RECEIVES & SENDS REPORTS ON FRAUD INCIDENTS (FRAUD & SCAM) FROM/TO NETWORK PARTICIPANTS, INCLUSIVE OF FRAUD CATEGORY

Zelle® categorizes Fraud in two primary ways:

- **fraud**: An *unauthorized* transfer of funds. Typically involves a takeover of the victim's account, perhaps via social engineering or ID/PW compromises. Examples include phishing, vishing, etc.
- **Scams**: An *authorized* transfer of funds. Typically involves the victim willingly sending money in response to a solicitation on the internet to purchase or receive goods/services. Examples include fake ticket sales, romance scams, etc.

Third Party Fraud
Unauthorized

Account Takeover (001)
Elder Abuse (006)
Friendly Fraud (007)
Social Engineering (008)
Third Party Fraud (009)
Identity Takeover (011)

Scam
Authorized

Scam – Other (005)
Scam – Charity (024)
Scam – Imposter (025)
Scam – Investment (026)
Scam – Merchandise (027)
Scam – Jobs (028)
Scam – Property (029)
Scam – Romance (030)

Out of Network Fraud
Unauthorized

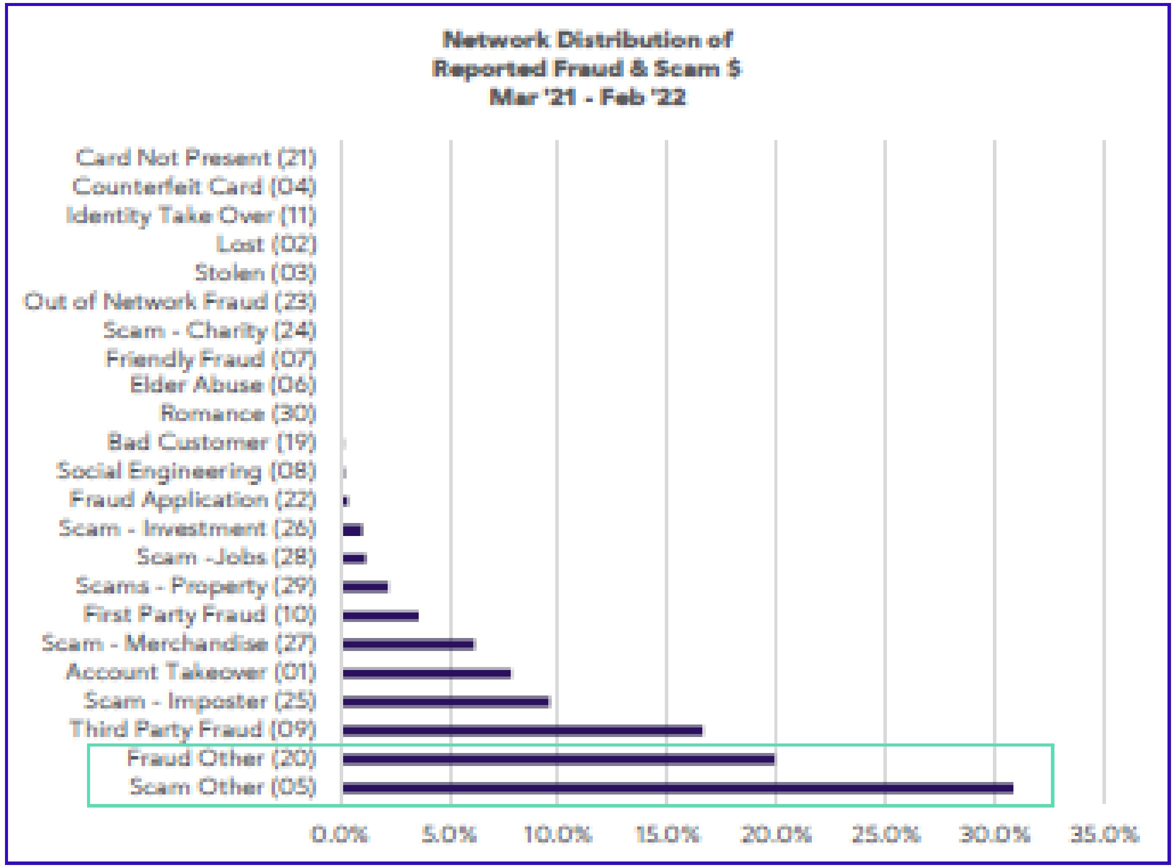
Out of Network Fraud (023)

First Party Fraud
Authorized

First Party Fraud (010)
Bad Customer (019)

1. Definitions for each fraud / Scam category located in Appendix

CONTEXT: Current Fraud Types Reported by Network

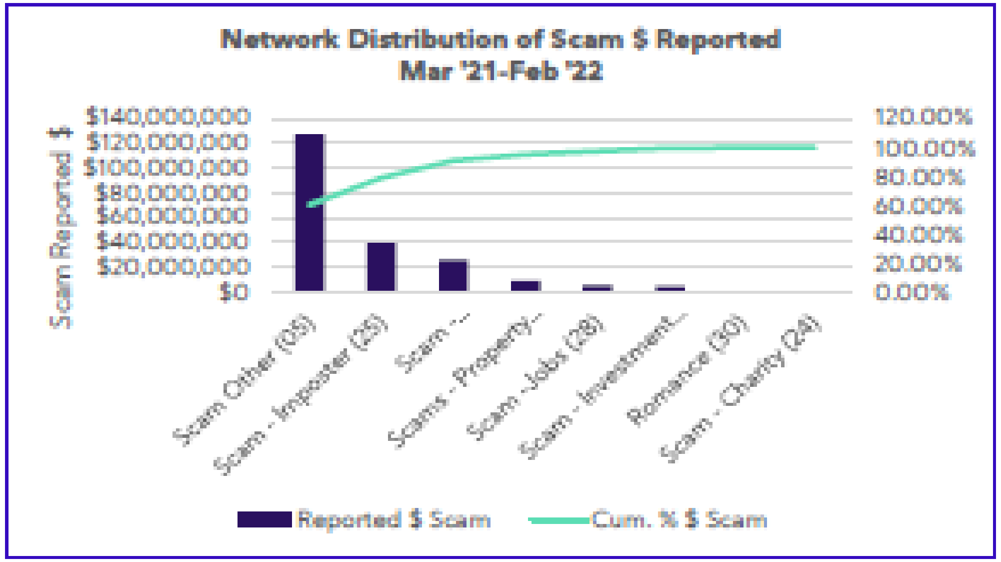


Breakout of fraud/scams reported from March '21 – February '22

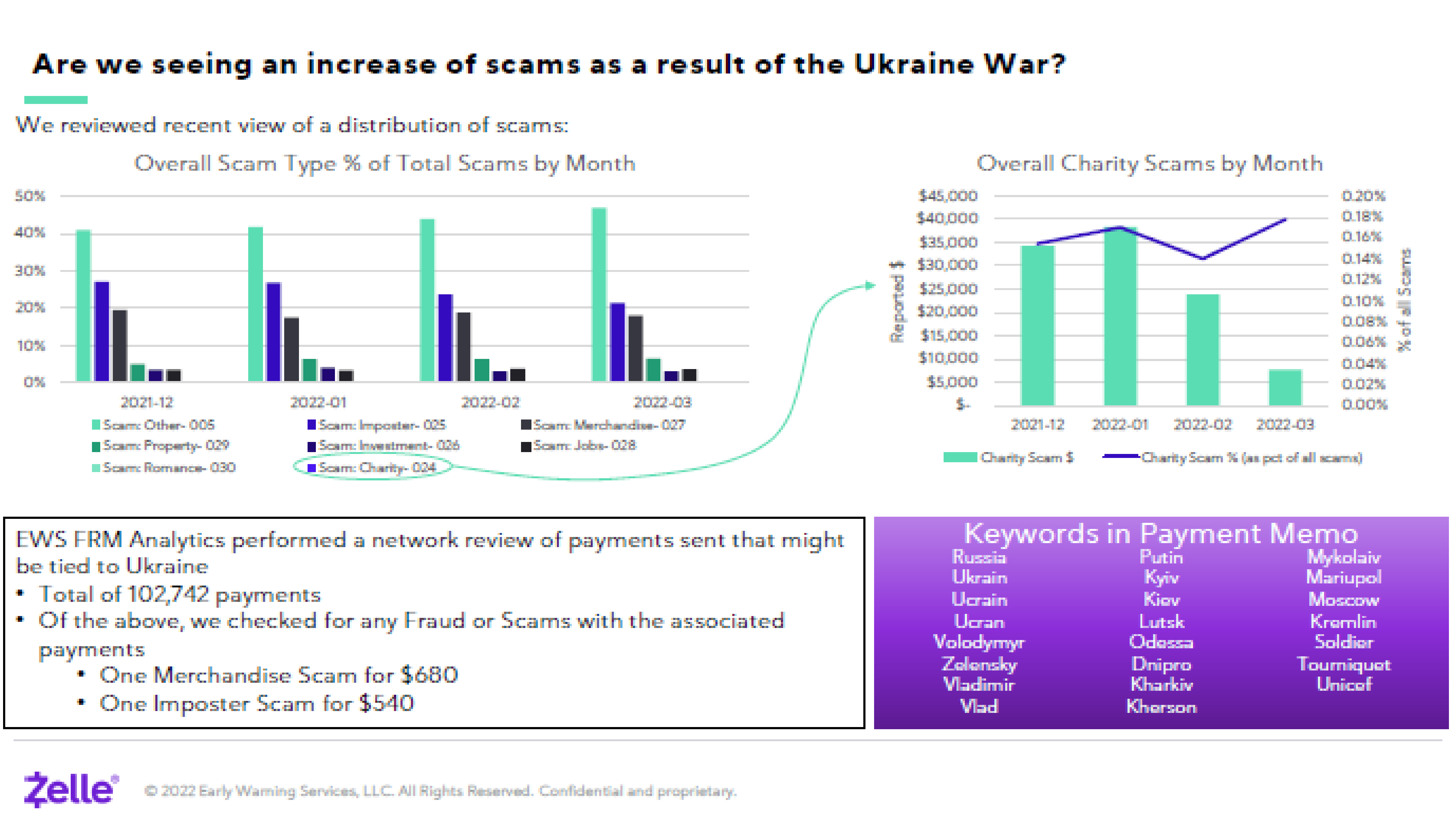
- 31% of reported items are generically classified as Scam (Other)
- 20% of reported items are generically classified as Fraud (Other).

Effective April '22 Fraud type Other is being retired as a valid Fraud Type in order improve classifications.

- 60% of all scams reported are classified as Scam (Other)



Fraud types 002, 003, 004, 022, 020, 021 no longer valid after April 2022



Are we seeing an increase of scams as a result of the Ukraine War?

We reviewed recent view of a distribution of scams:

EWS FRM Analytics performed a network review of payments sent that might be tied to Ukraine

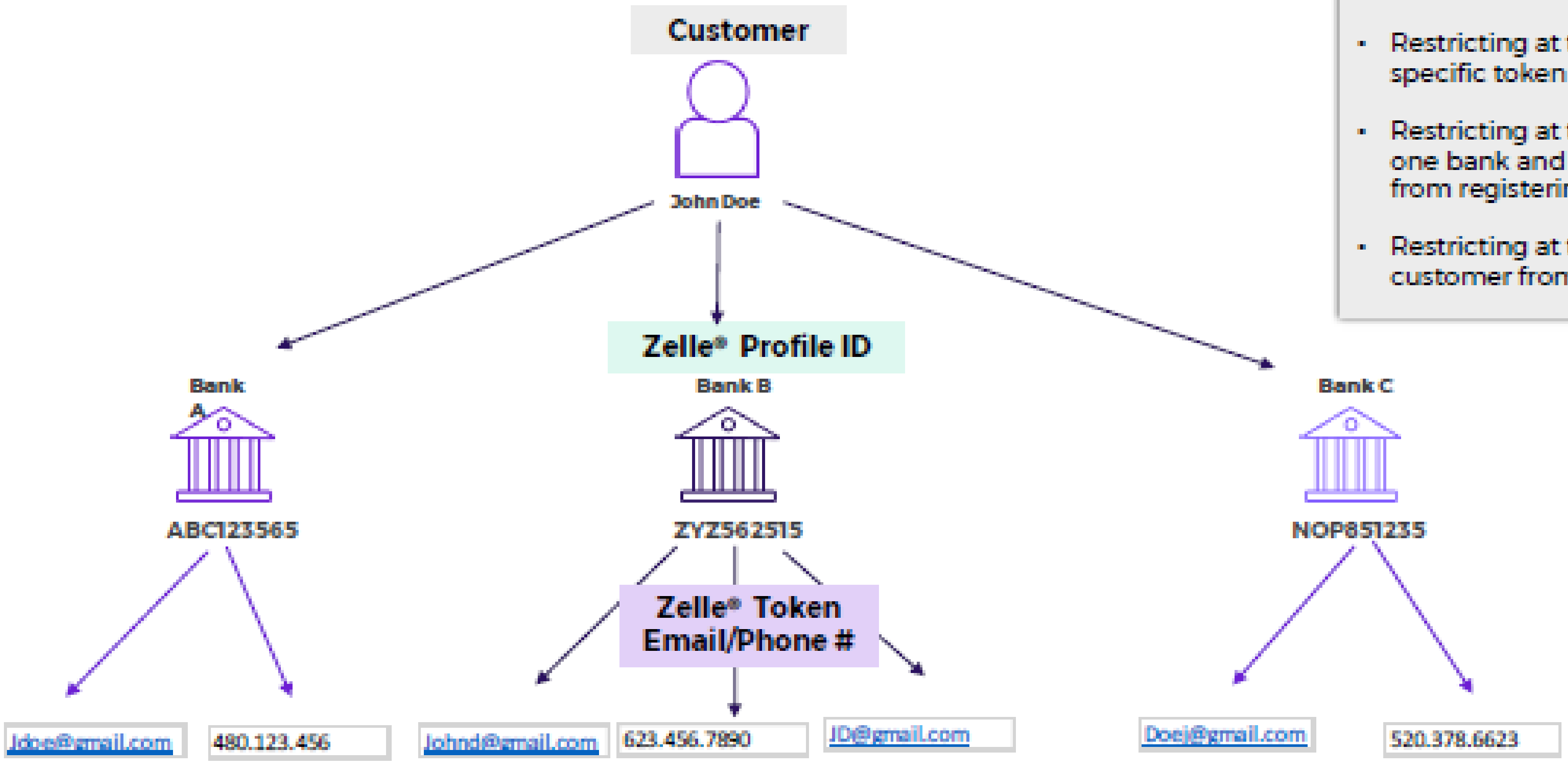
- Total of 102,742 payments
- Of the above, we checked for any Fraud or Scams with the associated payments
  - One Merchandise Scam for $680
  - One Imposter Scam for $540

Keywords in Payment Memo

Russia	Putin	Mykolaiv
Ukrain	Kyiv	Mariupol
Ucrain	Kiev	Moscow
Ucran	Lutsk	Kremlin
Volodymyr	Odessa	Soldier
Zelensky	Dnipro	Tourniquet
Vladimir	Kharkiv	Unicef
Vlad	Kherson	

Zelle

Context setting: registration/restriction at various tiers in network



Customer

John Doe

Zelle® Profile ID

Bank A

Bank B

Bank C

ABC123565

ZYZ562515

NOP851235

Zelle® Token Email/Phone #

Jdoe@gmail.com

480.123.456

Johnd@gmail.com

623.456.7890

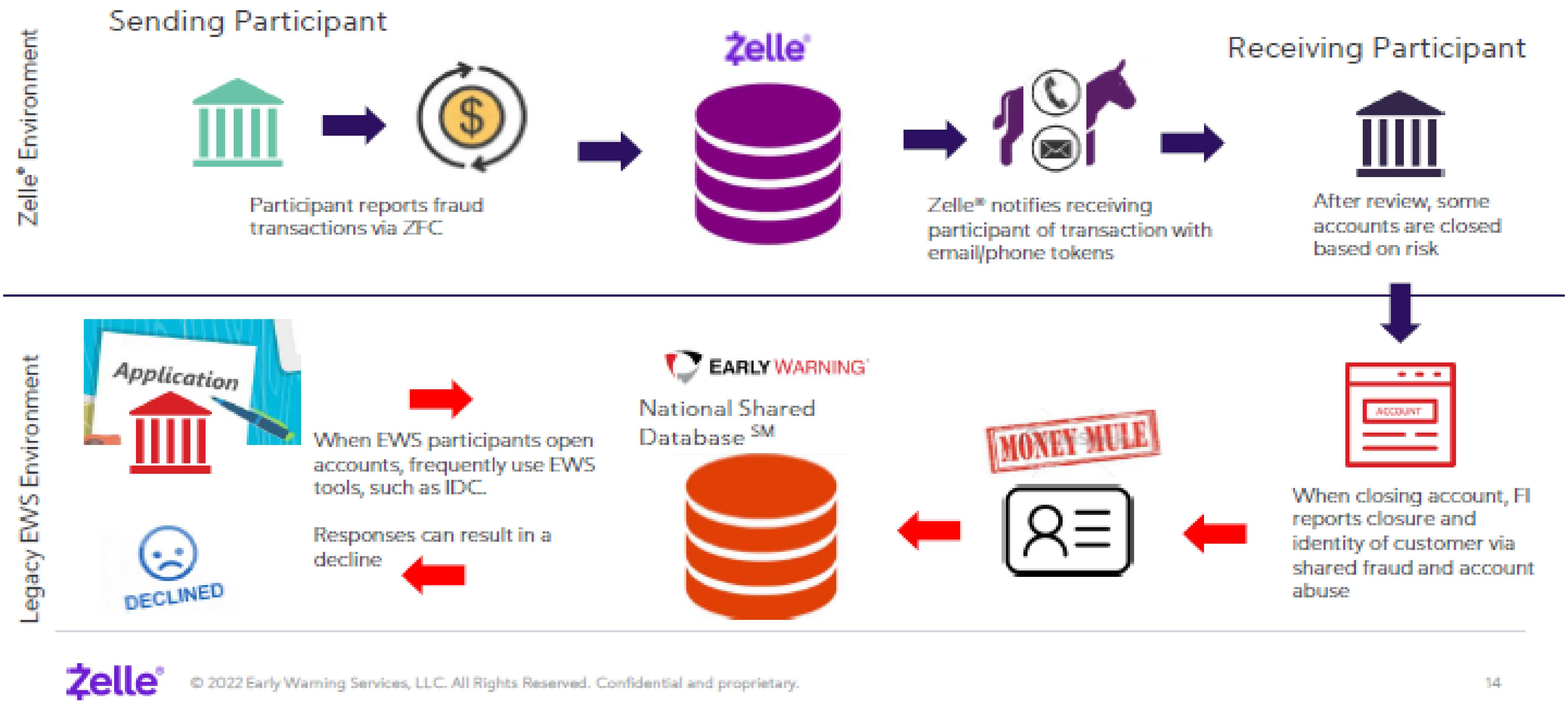
JD@gmail.com

Doej@gmail.com

520.378.6623

- One customer who banks with 3 different FIs appears as 3 different customer profiles in the Zelle® Network
- Restricting at the token level only prevents that specific token from being used in the Network
- Restricting at the profile level, restricts the customer at one bank and all the tokens associated with the profile from registering elsewhere in the Network.
- Restricting at the customer level – prevents the customer from registering at any FI

HOW TO LEVERAGE ZELLE® / EWS TOOLS TO BLOCK THE BAD ACTING "PERSON" FROM ENGAGING IN THE ZELLE® NETWORK



Zelle® Environment

Sending Participant

Participant reports fraud transactions via ZFC

Zelle®

Zelle® notifies receiving participant of transaction with email/phone tokens

Receiving Participant

After review, some accounts are closed based on risk

Legacy EWS Environment

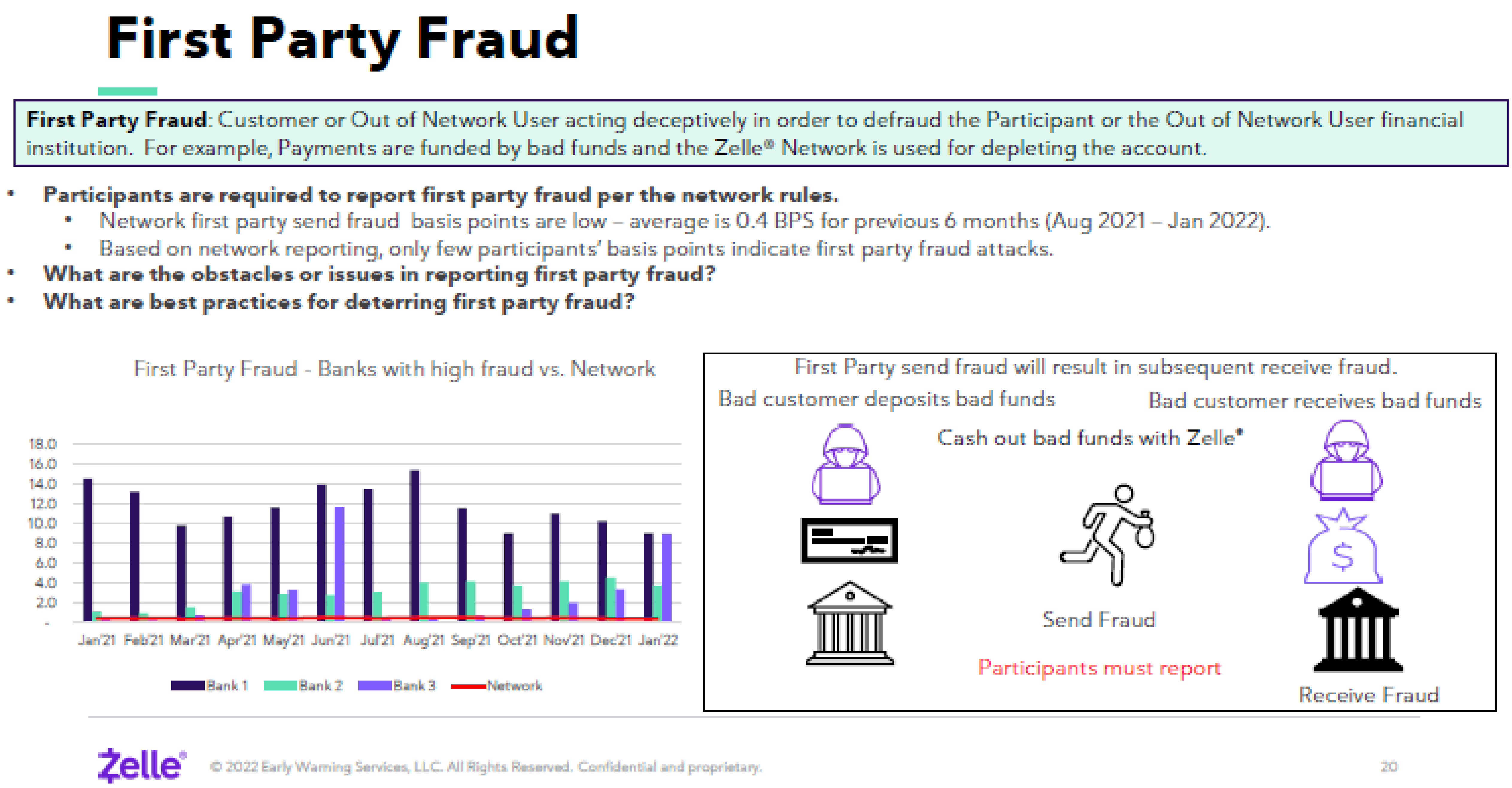
When EWS participants open accounts, frequently use EWS tools, such as IDC.

Responses can result in a decline

EARLY WARNING®

National Shared Database SM

When closing account, FI reports closure and identity of customer via shared fraud and account abuse



First Party Fraud

First Party Fraud: Customer or Out of Network User acting deceptively in order to defraud the Participant or the Out of Network User financial institution. For example, Payments are funded by bad funds and the Zelle® Network is used for depleting the account.

- **Participants are required to report first party fraud per the network rules.**
  - Network first party send fraud basis points are low – average is 0.4 BPS for previous 6 months (Aug 2021 – Jan 2022).
  - Based on network reporting, only few participants' basis points indicate first party fraud attacks.
- **What are the obstacles or issues in reporting first party fraud?**
- **What are best practices for deterring first party fraud?**

First Party Fraud - Banks with high fraud vs. Network

First Party send fraud will result in subsequent receive fraud.

Bad customer deposits bad funds
Bad customer receives bad funds
Cash out bad funds with Zelle®
Send Fraud
Participants must report
Receive Fraud

Zelle®

20

Align your reporting with these Fraud Types for April 2022

Fraud category	Fraud type code	Fraud type name	Description
Third party fraud (unauthorized)	001	Account Takeover	Customer's DDA or credentials have been compromised by fraudster.
	006	Elder Abuse	Elderly customer was taken advantage of and fraud occurred.
	007	Friendly Fraud	Fraud was committee by a friend or family member of the customer.
	008	Social Engineering	Use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
	009	Third Party Fraud	Customer has no knowledge of the payment. This unauthorized activity could be due to account takeover, identity theft, or any other type of unauthorized payment. **Note**: Fraud type code "009" must be used for third party fraud activity that cannot be clearly categorized
	011	Identity Take-Over (ITO)	Fraud as a result of a customer whose identity (SSN and other customer information) has been taken over for an unauthorized payment.
First party fraud	010	First Party Fraud	Customer acting deceptively in order to defraud the participant. For example, payments are funded by bad funds and the Zelle® Network is used for depleting the account. **Note**: Fraud type code "010" must be used for first party fraud activity that cannot be clearly categorized.
	019	Bad Customer	The customer has transacted in a manner that violates the terms of the participant's customer agreement.
OON chargeback	023	OON Chargeback	An issuing bank has issued a fraud chargeback to a Zelle® participant for a payment which was sent via the Zelle® app.
Scam (authorized)	024	Scam - Charity	Spoof existing charities or pretend to be a non-profit.
	025	Scam - Imposter	Someone pretending to be a well-known business, family/friend or government agency.
	026	Scam - Investment	Get rich quick schemes.
	027	Scam - Merchandise	Offer to provide goods or services while providing nothing in return.
	028	Scam - Jobs	Promise of jobs that don't exist and require consumer to pay fees, purchase equipment, etc.
	029	Scam - Property	Sell or rent property the scammer does not own.
	030	Scam - Romance	Request for money under the guise of a romantic relationship.
	005	Scam - Other	Customer authorized a payment that was induced by, initiated, or sent as a result of a deceptive act by the recipient. **Note**: Scam type code "005" must be used for scam activity that cannot be clearly categorized.

Zelle Fraud Trends

Summary

Zelle turnkey fraud chargeback in Q1’22 is at about 5 bps. Q4’22 Chargeback was 4 bps. Total fraud loss (fraud & scam) in Q1 is about 12.48 bps.

Large number of transactions from IP carrier - african network information center
Anomalous email domains: zetmail.com, candassociates.com, cutradition.com

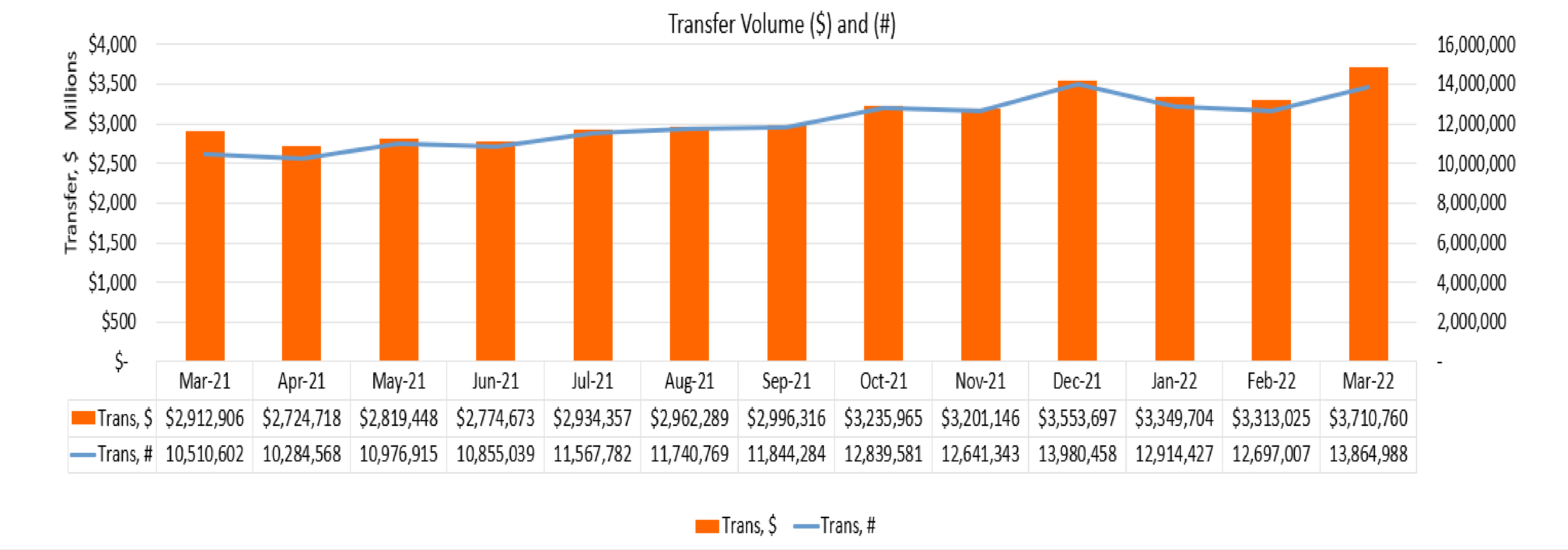
Suspending receiver contacts with high risk/disposable email domains

Scams continue to target users. About 55-60% of losses is from scams

Call Center override losses about 30% and SMS/OTP pass is 50%of total losses

Common App In network chargeback is 4.6bps in Apr.
Common App OON chargeback is about 35 bps in Apr.

Zelle Monthly Transaction Volumes

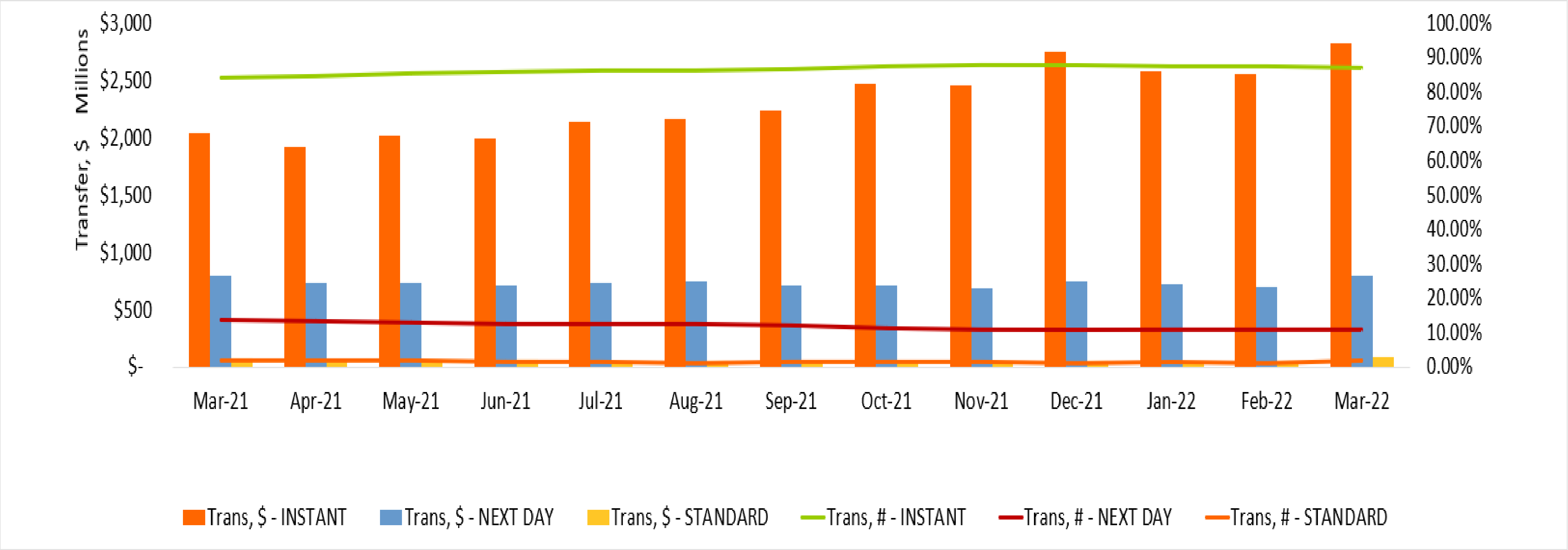


	Mar-21	Apr-21	May-21	Jun-21	Jul-21	Aug-21	Sep-21	Oct-21	Nov-21	Dec-21	Jan-22	Feb-22	Mar-22
▬ Trans, $	$2,912,906	$2,724,718	$2,819,448	$2,774,673	$2,934,357	$2,962,289	$2,996,316	$3,235,965	$3,201,146	$3,553,697	$3,349,704	$3,313,025	$3,710,760
— Trans, #	10,510,602	10,284,568	10,976,915	10,855,039	11,567,782	11,740,769	11,844,284	12,839,581	12,641,343	13,980,458	12,914,427	12,697,007	13,864,988

Data through Apr 4th , 2022

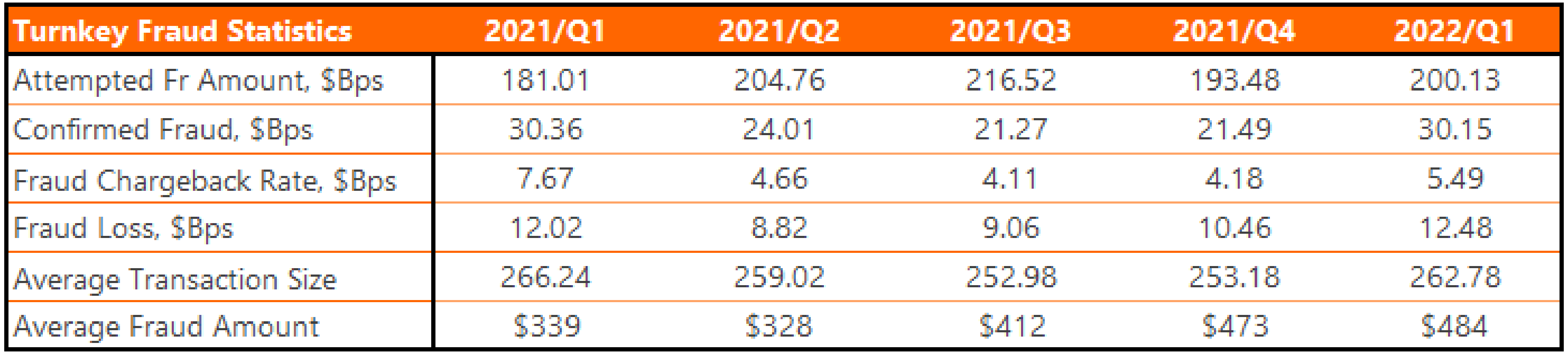
Transaction Distribution By Transfer Speed

88% of all transactions are instant, 11% is next day and 1% is standard speed



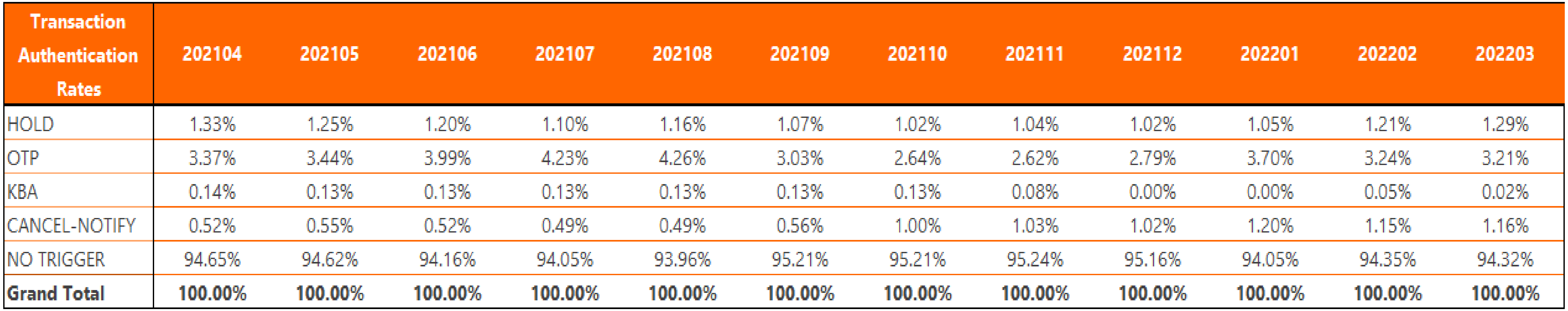
Fiserv Zelle Turnkey Risk Performance Stats

Fraud Losses in Q1’22 is about 13 bps. 50+% of losses reported are scams



Turnkey Fraud Statistics	2021/Q1	2021/Q2	2021/Q3	2021/Q4	2022/Q1
Attempted Fr Amount, $Bps	181.01	204.76	216.52	193.48	200.13
Confirmed Fraud, $Bps	30.36	24.01	21.27	21.49	30.15
Fraud Chargeback Rate, $Bps	7.67	4.66	4.11	4.18	5.49
Fraud Loss, $Bps	12.02	8.82	9.06	10.46	12.48
Average Transaction Size	266.24	259.02	252.98	253.18	262.78
Average Fraud Amount	$339	$328	$412	$473	$484

About 94% of transactions are allowed with no challenge. Hold rates are down consistent to reduce friction

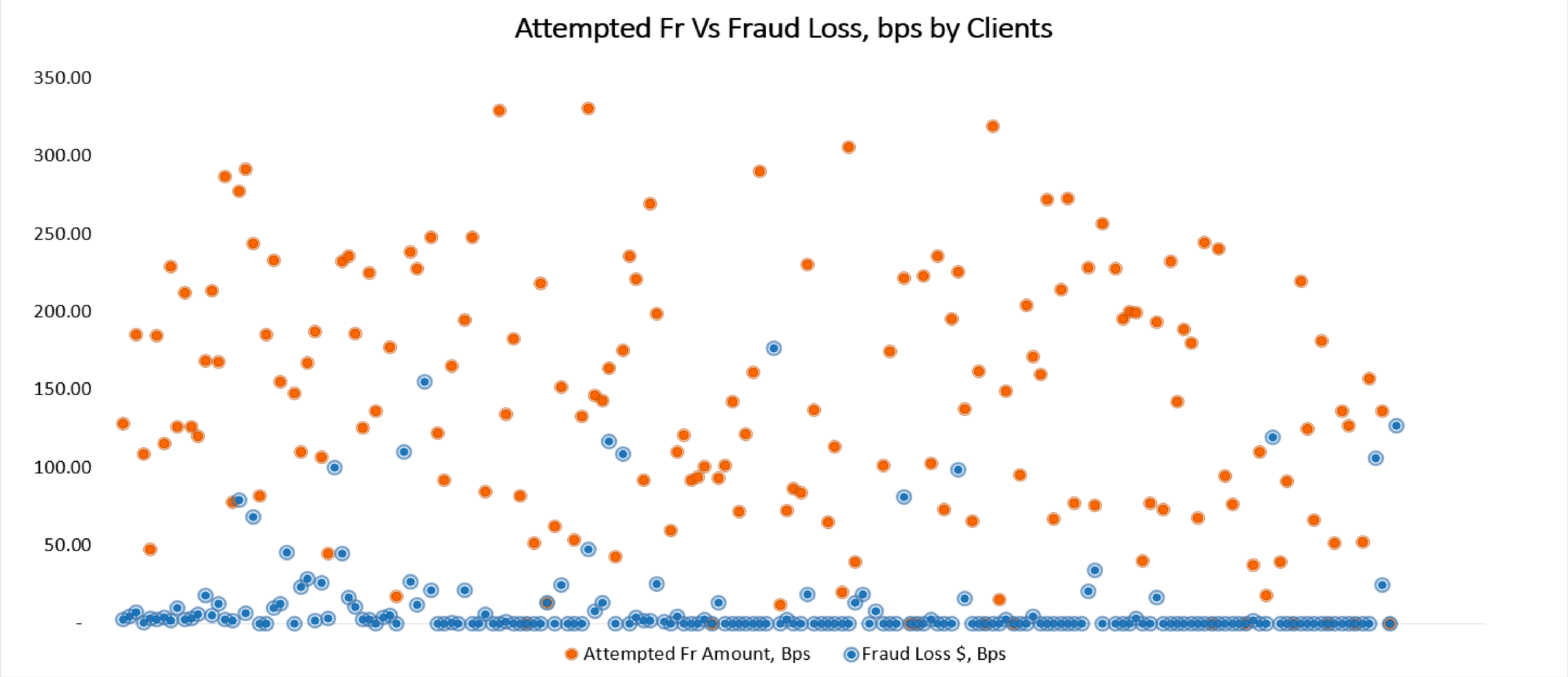


Transaction Authentication Rates	202104	202105	202106	202107	202108	202109	202110	202111	202112	202201	202202	202203
HOLD	1.33%	1.25%	1.20%	1.10%	1.16%	1.07%	1.02%	1.04%	1.02%	1.05%	1.21%	1.29%
OTP	3.37%	3.44%	3.99%	4.23%	4.26%	3.03%	2.64%	2.62%	2.79%	3.70%	3.24%	3.21%
KBA	0.14%	0.13%	0.13%	0.13%	0.13%	0.13%	0.13%	0.08%	0.00%	0.00%	0.05%	0.02%
CANCEL-NOTIFY	0.52%	0.55%	0.52%	0.49%	0.49%	0.56%	1.00%	1.03%	1.02%	1.20%	1.15%	1.16%
NO TRIGGER	94.65%	94.62%	94.16%	94.05%	93.96%	95.21%	95.21%	95.24%	95.16%	94.05%	94.35%	94.32%
Grand Total	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**

Fraud loss definition Includes confirmed fraud transaction (chargeback and Compass suspension where credit was released. Unconfirmed fraud is excluded

Fiserv Zelle Turnkey - Attempted Fraud and Fraud Loss by Client

Majority of clients continue to see less than 15bps of fraud in March' 2022

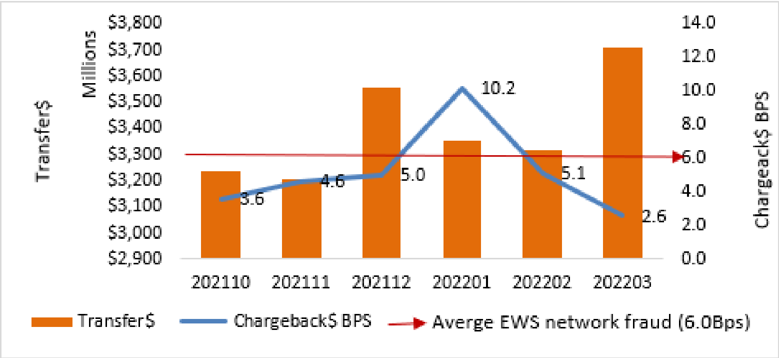


Client →

Period: Mar. 2022

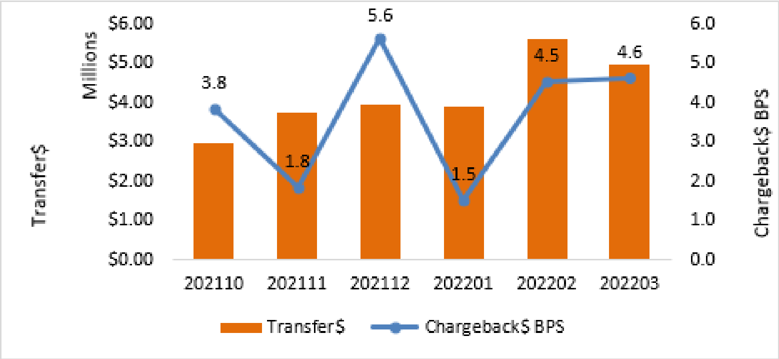
Zelle Fraud Chargeback Trends (Turnkey, CMA and OON)

Fiserv **Turnkey Client** Losses



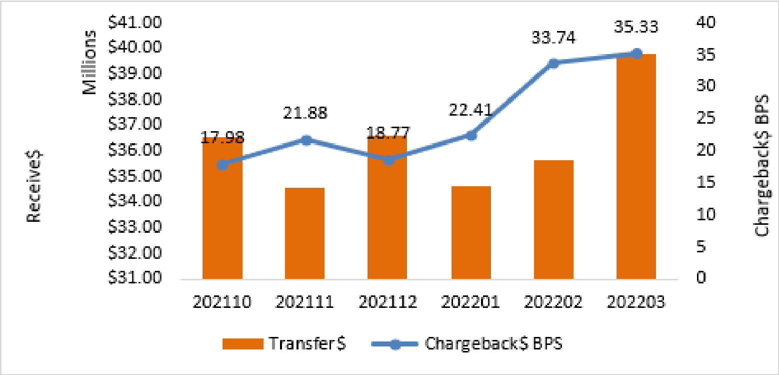
- Zelle turnkey chargebacks dropped to 2.6 bps in Mar.
- Zelle overall fraud losses is 6.3 bps in Mar.

Fiserv Clients **Zelle CMA** Losses



- CMA In-network volumes are averaging $4.1M from Oct-Mar.
- CMA In-network fraud averaging 3.7bps over last 6 months.

Fiserv Clients **Zelle OON** Losses



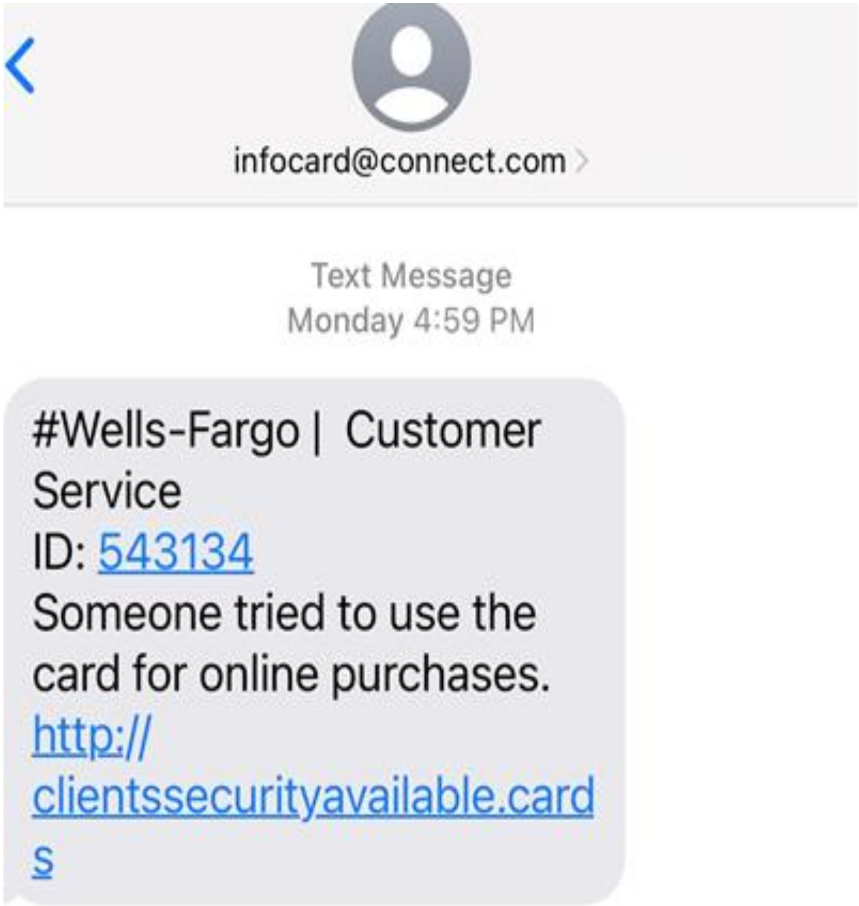
- CMA Out-of-network transaction volume average about $36M/month .
- CMA Out-of-network fraud is 35bps in Mar.

Open Discussion

- Scam Trends: What scams are you seeing? Puppy, Merchandise, COVID, Tax?
  - One large FI experiencing remote access fraud
  - Elders are getting scammed at higher rate
  - Refund scams are continuing to target clients.
  - Self Pay scams
  - Stay at home MLM businesses employment scams
- Fraud trends: What trends are you seeing recently. Account take over. First Party, New account? Smishing attacks? RATs?

Appendix

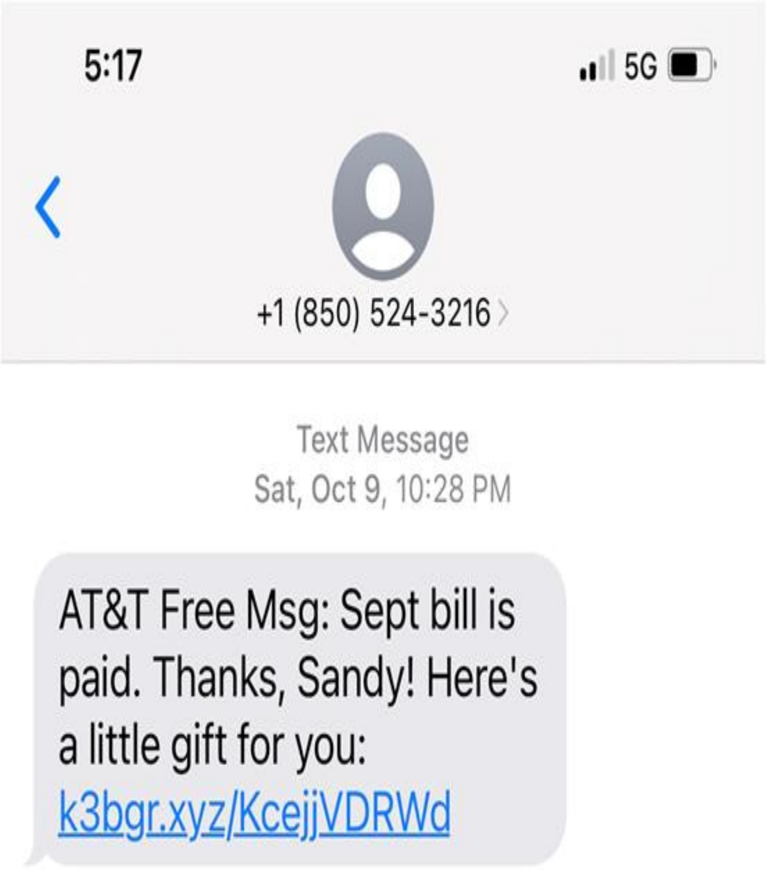
Sample of Scam Txts



infocard@connect.com

Text Message
Monday 4:59 PM

#Wells-Fargo | Customer Service
ID: 543134
Someone tried to use the card for online purchases.
http://clientssecurityavailable.cards



+1 (850) 524-3216

Text Message
Sat, Oct 9, 10:28 PM

AT&T Free Msg: Sept bill is paid. Thanks, Sandy! Here's a little gift for you: k3bgr.xyz/KcejjVDRWd

Consumer Education Recommendations in OLB

We recommend that you remind your consumers of the importance of protecting their bank accounts by following these tips and best practices. The following scam notifications are suggested to be displayed at a prominent location on your website:

- Refunds are not issued through Zelle
- Your financial institution will never call you to request information you received via text (SMS) or pressure you to reset your online banking log in password
- Don’t trust caller ID; Caller ID could be spoofed to show your financial institution’s name
- Don’t provide your online banking log in credentials, one-time password, account number or personal information by email or text or phone call. Using their published phone number, reach out to your financial institution to confirm that the request is legitimate
- Don’t give information over the phone if you receive a call stating that a transaction is canceled, even if the caller claims to be from your financial institution. Once again, contact your financial institution using a published phone number to inquire about the transaction
- Don’t click on links in unsolicited emails or texts
- Don’t give an unsolicited caller remote access to your computer

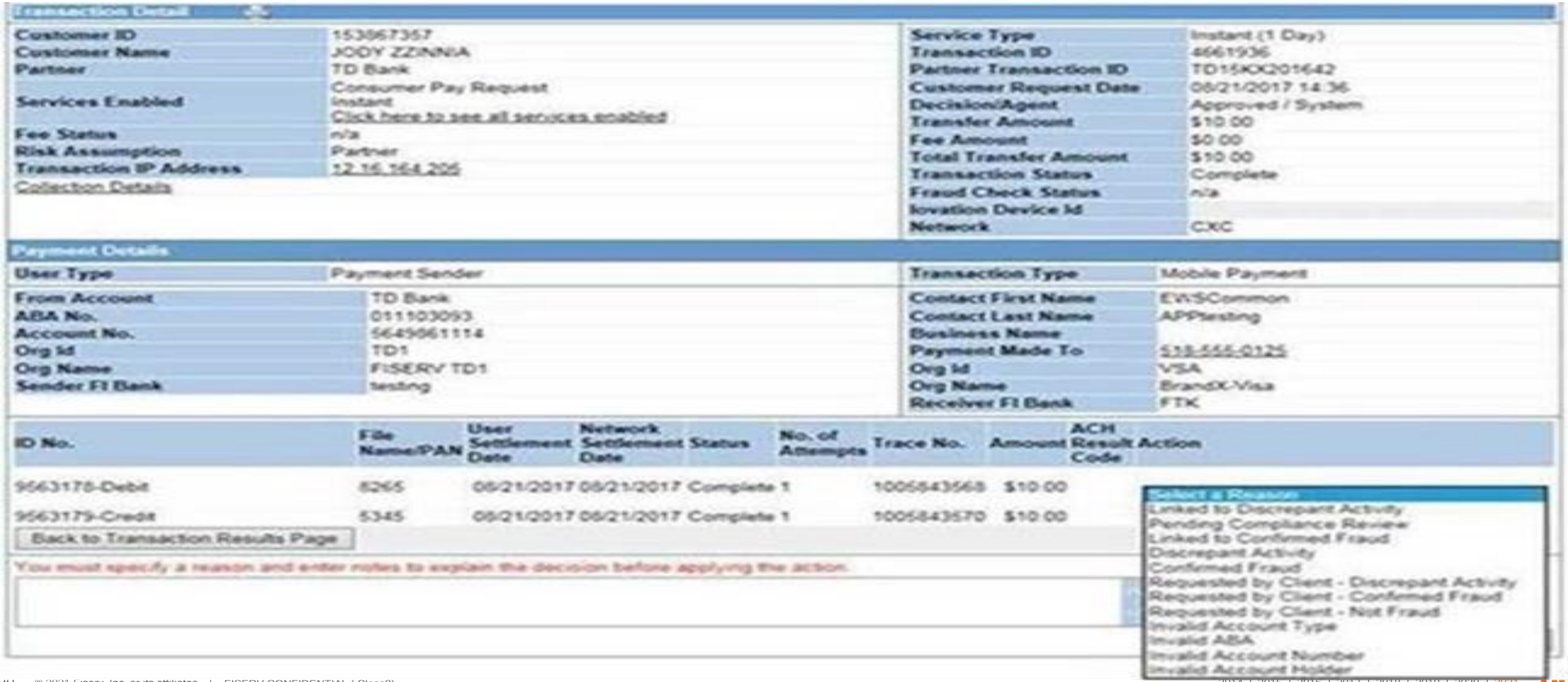
Fraud Dispute - How to identify Fraudulent P2P Claims

Its generally difficult to confirm if the user claiming fraud is a victim or is a party to it. However, you may evaluate the case based the following guiding factors:

- Tenure of the account and other relationships - Generally users with >6 months in books are good.
- Past transaction history at the bank – Users with good history do not call with frivolous claims
- Past history with the receiver account/token
- Recent activity of deposits and withdrawals
- Was the log-in from a new device?
- Was there a password reset or new login during recent months?
- Is the user willing to sign an affidavit of fraudulent activity?

Compass Screen to Report Fraud Disputes and Scams

In addition to chargeback information contributed by the FI, Fiserv will also contribute transactions that have been suspended as **Confirmed Fraud or Confirmed Scam** in the Risk Management screens in Compass. If the transaction has been canceled, you may mark transaction as **Discrepant activity**. Please refer to the compass screen below or refer to Compass UG.



Transaction Detail

Customer ID	153867357
Customer Name	JODY ZZINNIA
Partner	TD Bank
Services Enabled	Consumer Pay Request Instant Click here to see all services enabled
Fee Status	n/a
Risk Assumption	Partner
Transaction IP Address	12.16.164.205

Collection Details

Service Type	Instant (1 Day)
Transaction ID	4661936
Partner Transaction ID	TD15KX201642
Customer Request Date	08/21/2017 14:36
Decision/Agent	Approved / System
Transfer Amount	$10.00
Fee Amount	$0.00
Total Transfer Amount	$10.00
Transaction Status	Complete
Fraud Check Status	n/a
Iovation Device Id	
Network	CXC

Payment Details

User Type	Payment Sender
From Account	TD Bank
ABA No.	011103093
Account No.	5649961114
Org Id	TD1
Org Name	FISERV TD1
Sender FI Bank	testing

Transaction Type	Mobile Payment
Contact First Name	EWSCommon
Contact Last Name	APPtesting
Business Name	
Payment Made To	518-555-0125
Org Id	VSA
Org Name	BrandX-Visa
Receiver FI Bank	FTK

ID No.	File Name/PAN	User Settlement Date	Network Settlement Date	Status	No. of Attempts	Trace No.	Amount	ACH Result Code	Action
9563178-Debit	8265	08/21/2017	08/21/2017	Complete	1	1005843568	$10.00		
9563179-Credit	5345	08/21/2017	08/21/2017	Complete	1	1005843570	$10.00		

You must specify a reason and enter notes to explain the decision before applying the action.

Back to Transaction Results Page
Select a Reason
Linked to Discrepant Activity
Pending Compliance Review
Linked to Confirmed Fraud
Discrepant Activity
Confirmed Fraud
Requested by Client - Discrepant Activity
Requested by Client - Confirmed Fraud
Requested by Client - Not Fraud
Invalid Account Type
Invalid ABA
Invalid Account Number
Invalid Account Holder