1st Party Trust

Patrick Kelly, Mastercard

Linda Van Horn, Direct Trust

Moderator: Deb Ferril, ASCEND

IDENTITY & PAYMENTS SUMMIT

What is First Party Fraud?

In payments, First-party fraud occurs when a consumer makes a legitimate purchase and then later requests a chargeback, even though the goods or services were received.

IDENTITY & PAYMENTS SUMMIT

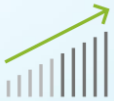
42% of Gen Z

admit to engaging in first-party fraud

IDENTITY & PAYMENTS SUMMIT

Source: Fast Company article (Sift)

What is fueling First Party Fraud ?



Increased ecommerce shopping

Ease of dispute process

Difficult to detect first party fraud activity

Zero fraud liability consumer awareness

Consumer protective regulations

Issuer lacks data and insights

First Party Fraud

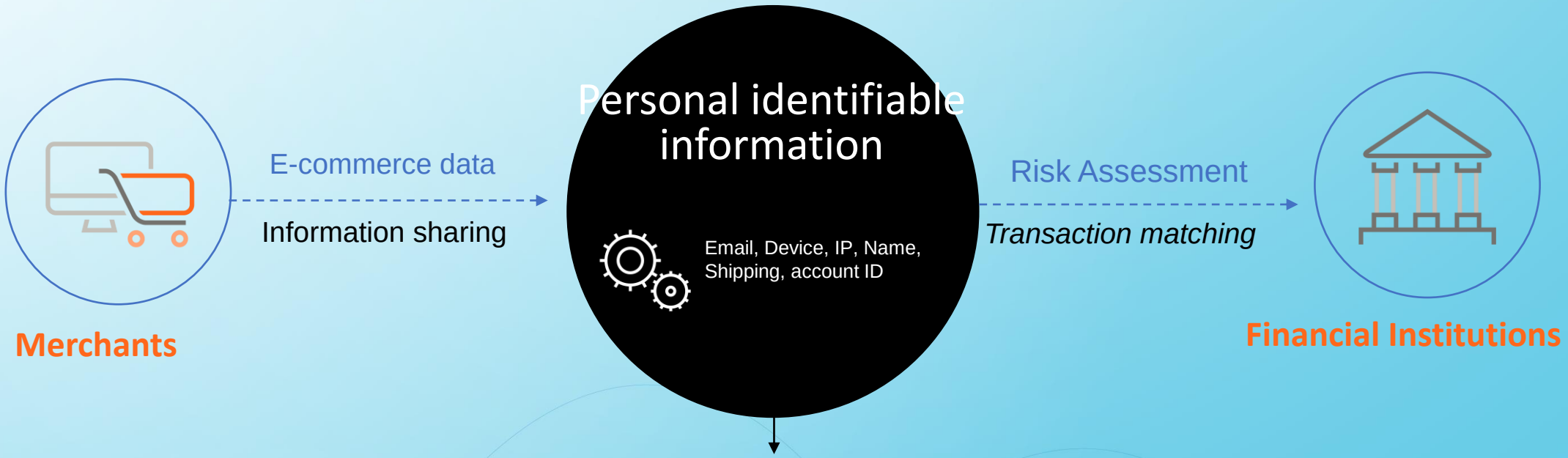
$100B

…problem for businesses

Fast Company (2024)

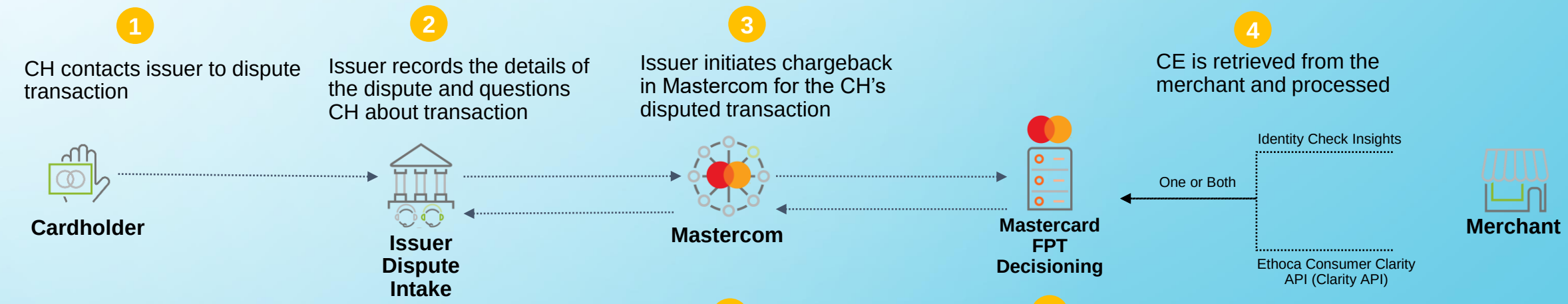
IDENTITY & PAYMENTS SUMMIT

Most fraud is a data problem..



IDENTITY & PAYMENTS SUMMIT

A future look at First Party Fraud remediation



8
Issuer discusses dispute status with CH and decides how to proceed.

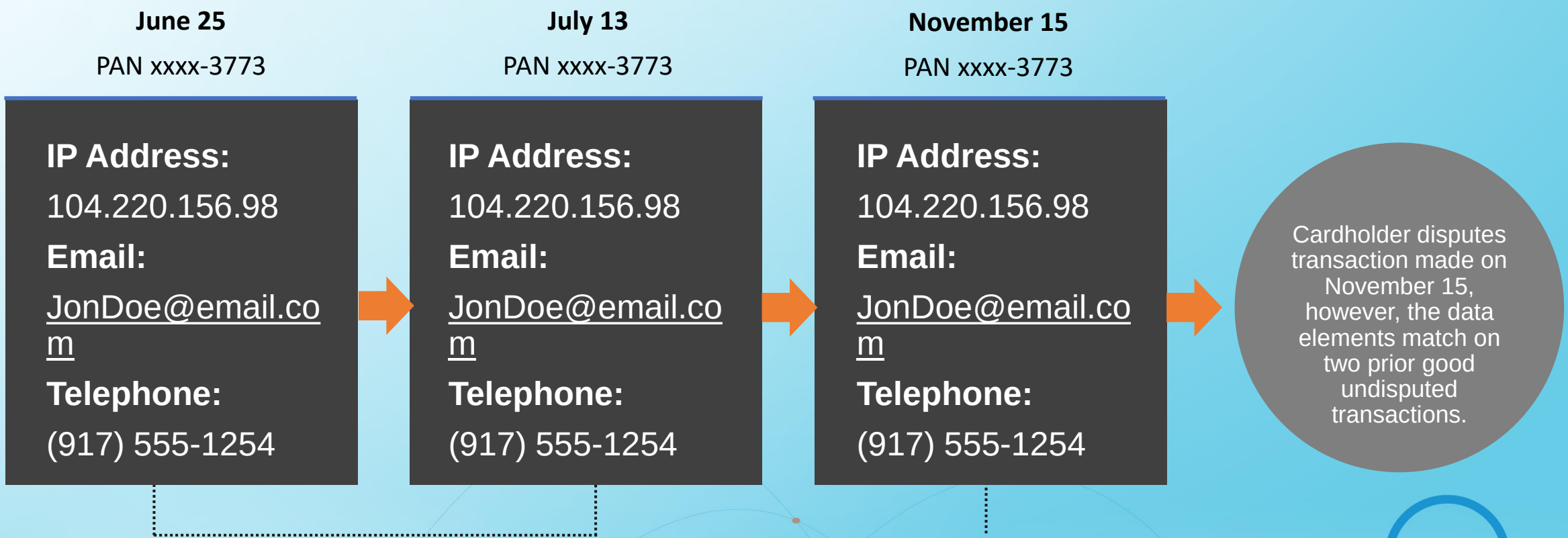
7
Issuer view CE in Clarity Call Center directly or via Mastercom link

6
Mastercom rejects the CB back to the issuer with 5002 error.

5
Mastercard validates the CE, confirms first party fraud.

IDENTITY & PAYMENTS SUMMIT

First Party Trust – Data Matching Example



IDENTITY & PAYMENTS SUMMIT

What's next?

- Optional Merchant Program (requires merchant to enroll and opt-in)
- Issuer's cannot opt-out – must process new FPT reason code
- US 50 States Only – Both the merchant and issuer are in the US

2024

October 23rd

Announcement Published – AN 8364

Q1 2024

Offline Data Studies with Merchants and Issuers

2024

Q3 2024

Live transaction testing

October 2024

Program Effective

IDENTITY & PAYMENTS SUMMIT

Identity Theft in Healthcare

Presenter: Linda Van Horn, BS, MBA

President/CEO iShare Medical

IDENTITY & PAYMENTS SUMMIT

Linda Van Horn, BS, MBA

iShare Medical®

Founder, President / CEO

- Health Care and IT Expert and Serial Entrepreneur
- Former DirectTrust Executive Board Members
- Voting Member of 4 ANSI Consensus Bodies
  - Direct Standard™
  - TIM+ Standard
  - Notifications via Direct Standard
  - Privacy Enhancing Record Locator Service

Prior Experience

21st Century Edge | Founder

The Pain Institute | Co-Founder

Deloitte | Senior Manager IT Consulting & Development

IDENTITY & PAYMENTS SUMMIT

iShare Medical®

iShare Medical is the trusted online platform for identity, interoperability, integration, and automation of workflow for patients, providers, payers, and devices to share medical records across our nationwide network of 2.8 million providers.

IDENTITY & PAYMENTS SUMMIT

iShare Medical is a DirectTrust Accredited Trust Anchor

This presentation will discuss DirectTrust, a non-profit trade association, that consists of:

- Trust Frameworks: one for nationwide provider and payer identity and interoperability in healthcare and another is SAFE Identity for bio-pharma
- Accreditation body operated under the name of EHNAC
- ANSI Standards Development Organization

IDENTITY & PAYMENTS SUMMIT

Identity Theft in Healthcare Agenda

- About the Speaker and DirectTrust
- Medical Identity Theft
- Definition: Identity Theft in Healthcare
- DirectTrust Framework Digital Identity Establishes Trust
- Four Examples of Attacks in 2023:
  1. Business Email Compromise (BEC) Phishing / Spoofing
  2. Counterfeit Drugs in the Supply Chain
  3. Digital Identity and Verification in the Supply Chain
  4. Inside Attack: Data Loss and Exfiltration is on the Rise
- How the DirectTrust Framework helps prevent these five attacks

IDENTITY & PAYMENTS SUMMIT

Medical Identity Theft

1.85M	Of the U.S. population were victims of medical identity theft.
$22.3K	Mean cost per incident of medical identity theft was $22,346.
$41.3B	Estimated annual cost of medical identity theft is the U.S. is **$41.3 billion**.
1 year	34% said it took one year or more to be notified of identity theft.

Source: Third Annual Survey on Medical Identity Theft Ponemon Institute June 2012

IDENTITY & PAYMENTS SUMMIT

Definition: Identity Theft in Healthcare

Identity theft in healthcare occurs when:

1) Someone uses your personal information such as your name, social security number, Medicare, or other health insurance information to claim to be you and then uses this information to fraudulently obtain medical care, prescription medications, government benefits, other goods and services in your name, or to get access to your medical records or

2) impersonates the identity of an individual, organization, or product to:

a) gain access to personal information of employees, protected health information, or other confidential data or

b) obtain payment or transfer of money based on false pretenses.

IDENTITY & PAYMENTS SUMMIT

DirectTrust Framework
Known Digital Identity Security and Trust

- Identity Proofing at NIST 800-63-3 IAL2 bound to the real persons identity in the form of a Verifiable Digital Trust Credential bound to two pairs of X.509 Certificates one for digital signature and the other for encryption
- Identity Authentication NIST 800-63-3 AAL2 on every login and every transaction regardless of whether or not the source is inside or outside the corporate firewalls
- You can not spoof or span a Direct Message as the sender and receiver are always known
- There is an audit trail of all transactions

IDENTITY & PAYMENTS SUMMIT

Business Email Compromise Phishing / Spoofing

54%

of healthcare organizations experienced an average of **five** BEC attacks in the 2023.

Business Email Compromise is a type of scam that relies heavily on social engineering tactics to trick unsuspecting employees and executives by impersonating identity of some individual or organization inside or outside of the business to obtain payment, transfer of money, personal information of employees, or protected health information via business email.

IDENTITY & PAYMENTS SUMMIT

Source: Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care
Ponemon Institute, sampling frame 17,085, final sample 653 or 3.8%

Counterfeit Drugs Are in the Supply Chain

10.5%

“The World Health Organization states the frightening figure in which almost 10.5% of the medications worldwide are either subpar or fake.”

In many cases, these drugs are purchased through legitimate medicine supply chains.

Source: Pathak R, Gaur V, Sankrityayan H, Gogtay J. Tackling Counterfeit Drugs: The Challenges and Possibilities. Pharmaceut Med. 2023 Jul;37(4):281-290. doi: 10.1007/s40290-023-00468-w. Epub 2023 May 15. PMID: 37188891; PMCID: PMC10184969.

IDENTITY & PAYMENTS SUMMIT

Organizations Unprepared to Stop Attacks that Impact Patient Care

69%

of healthcare organizations that had a BEC said that it disrupted patient care.

64%

of healthcare organizations had an average of four supply chain attacks in last two years.

55%

of healthcare organizations say they do **not** have a strategy to stop BEC and supply chain attacks.

Source: 2023 Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care
Ponemon Institute, sampling frame 17,085, final sample 653 or 3.8%

IDENTITY & PAYMENTS SUMMIT

How DirectTrust Trust Framework Prevents Email Phishing / Spoofing Attacks

- Identity Proofing at NIST 800-63-3 IAL2 and bound to the real persons identity in the form of a Verifiable Digital trust Credential (e.g. two X.509 Certificates one for digital signature and the other for encryption)
- Identity Authentication NIST 800-63-3 AAL2 on every login and every transaction regardless of whether or not the person is inside or outside the corporate firewalls

Prevented

- You cannot spoof or span a Direct Message as the sender and receiver are always known
- Maintain an audit trail of all transactions

IDENTITY & PAYMENTS SUMMIT

How DirectTrust Identity Prevents Counterfeit Drugs in Supply Chain

FDA Drug Supply Chain Security Act (DSCSA) outlines requirements to develop and enhance the drug supply chain security by November 27, 2024.

Prevented

a) Digital Identity - Drug traceability and verification
b) Digital Tracking - Drug distribution supply and distribution security
c) Digital Verification of Identity of the Drug - to protect patients from exposure to counterfeit, stolen, contaminated or otherwise harmful drugs

The above three items are a part of the DirectTrust SAFE Identity for bio-pharma Trust Framework.

IDENTITY & PAYMENTS SUMMIT

Inside Attack: Data Loss and Exfiltration is on the Rise

100%

Of healthcare organizations surveyed had at least one incident where sensitive healthcare data was lost or stolen.

Malicious insiders are the number one cause of data loss and exfiltration (the unauthorized transfer of information from a system).

Source: 2023 Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care
Ponemon Institute, sampling frame 17,085, final sample 653 or 3.8%

IDENTITY & PAYMENTS SUMMIT

Summary DirectTrust: Known Digital Identity Establishes Trust

- Identity Proofing at NIST 800-63-3 IAL2 and bound to the real persons identity in the form of a Verifiable Digital trust Credential (e.g. two X.509 Certificates one for digital signature and the other for encryption)

Detect Who →

- Identity Authentication NIST 800-63-3 AAL2 on every login and every transaction regardless of whether or not the person is inside or outside the corporate firewalls

- You can not spoof or span a Direct Message as the sender and receiver are always known

Track Who →

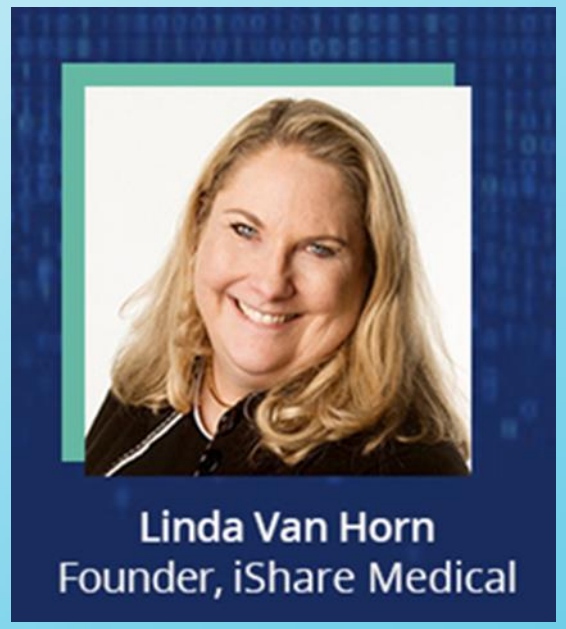
- Maintain an audit trail of all transactions

IDENTITY & PAYMENTS SUMMIT

Thank You!

iShare MEDICAL

INNOVATING THE FUTURE OF HEALTHCARE



Linda Van Horn
Founder, iShare Medical

@ l.vanhorn@isharemedical.com

816.249.2555 ext. 101

www.iShareMedical.com

IDENTITY & PAYMENTS SUMMIT