Fraud Trends

Mary Anne Colucci
Sr. Director Fraud & Risk
Envisant

August 2024

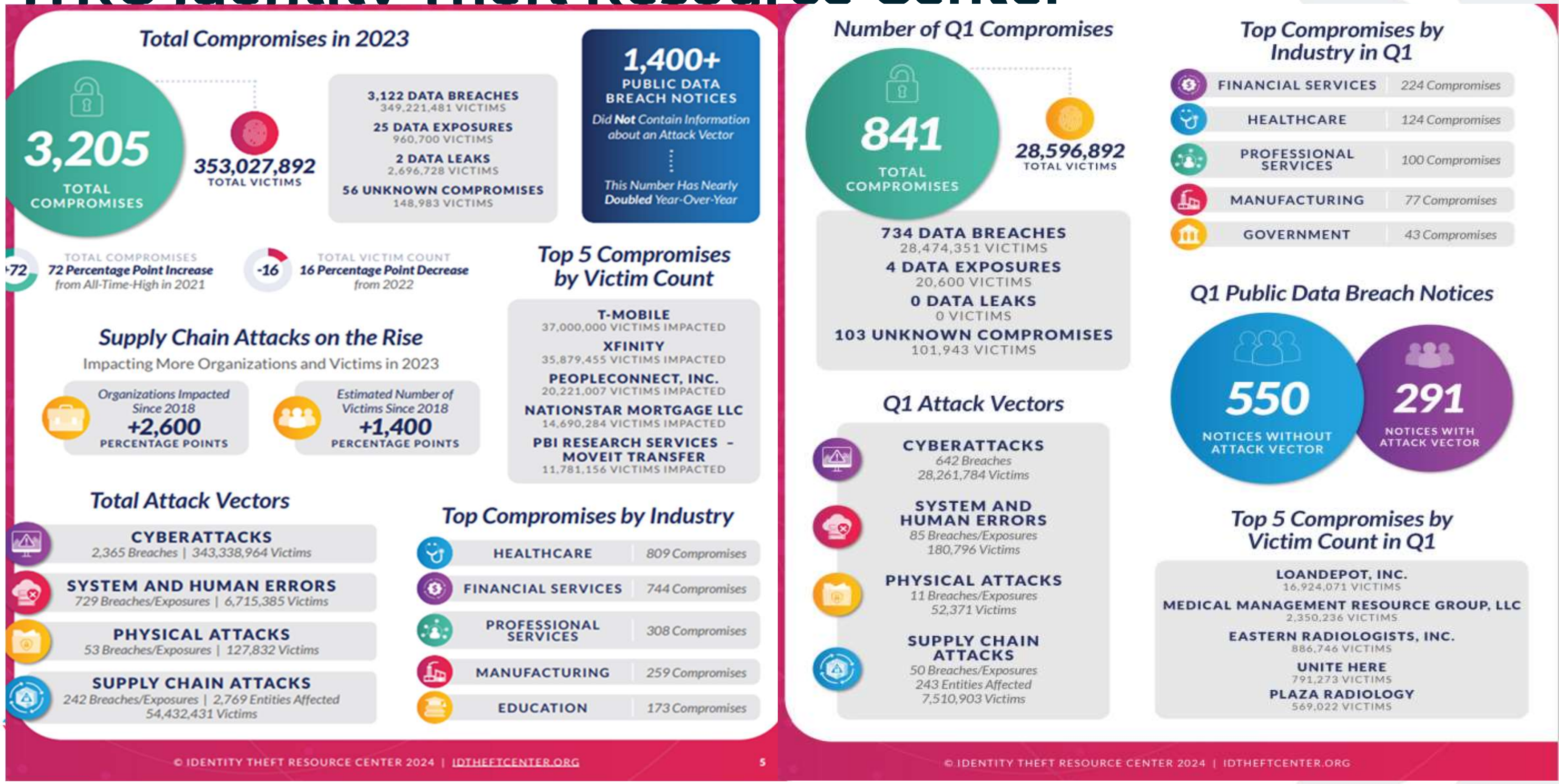
Envisant Achieve your **vision.**

Agenda

Overview	Slide 3
Imposter Scam	Slide 4
Enumeration and Testing	Slide 8
Ransomware	Slide 11
Other Common Trends	Slide 14
Artificial Intelligence	Slide 18

Envisant Achieve your **vision.**

ITRC Identity Theft Resource Center



Total Compromises in 2023

3,205 TOTAL COMPROMISES

353,027,892 TOTAL VICTIMS

3,122 DATA BREACHES
349,221,481 VICTIMS

25 DATA EXPOSURES
960,700 VICTIMS

2 DATA LEAKS
2,696,728 VICTIMS

56 UNKNOWN COMPROMISES
148,983 VICTIMS

1,400+
PUBLIC DATA BREACH NOTICES
*Did **Not** Contain Information about an Attack Vector*

*This Number Has Nearly **Doubled** Year-Over-Year*

+72 TOTAL COMPROMISES
72 Percentage Point Increase
from All-Time-High in 2021

-16 TOTAL VICTIM COUNT
16 Percentage Point Decrease
from 2022

Top 5 Compromises by Victim Count

T-MOBILE
37,000,000 VICTIMS IMPACTED

XFINITY
35,879,455 VICTIMS IMPACTED

PEOPLECONNECT, INC.
20,221,007 VICTIMS IMPACTED

NATIONSTAR MORTGAGE LLC
14,690,284 VICTIMS IMPACTED

PBI RESEARCH SERVICES – MOVEIT TRANSFER
11,781,156 VICTIMS IMPACTED

Supply Chain Attacks on the Rise

Impacting More Organizations and Victims in 2023

Organizations Impacted Since 2018
+2,600
PERCENTAGE POINTS

Estimated Number of Victims Since 2018
+1,400
PERCENTAGE POINTS

Total Attack Vectors

CYBERATTACKS
2,365 Breaches | 343,338,964 Victims

SYSTEM AND HUMAN ERRORS
729 Breaches/Exposures | 6,715,385 Victims

PHYSICAL ATTACKS
53 Breaches/Exposures | 127,832 Victims

SUPPLY CHAIN ATTACKS
242 Breaches/Exposures | 2,769 Entities Affected
54,432,431 Victims

Top Compromises by Industry

HEALTHCARE	*809 Compromises*
FINANCIAL SERVICES	*744 Compromises*
PROFESSIONAL SERVICES	*308 Compromises*
MANUFACTURING	*259 Compromises*
EDUCATION	*173 Compromises*

© IDENTITY THEFT RESOURCE CENTER 2024 | IDTHEFTCENTER.ORG

Number of Q1 Compromises

841 TOTAL COMPROMISES

28,596,892 TOTAL VICTIMS

734 DATA BREACHES
28,474,351 VICTIMS

4 DATA EXPOSURES
20,600 VICTIMS

0 DATA LEAKS
0 VICTIMS

103 UNKNOWN COMPROMISES
101,943 VICTIMS

Q1 Attack Vectors

CYBERATTACKS
642 Breaches
28,261,784 Victims

SYSTEM AND HUMAN ERRORS
85 Breaches/Exposures
180,796 Victims

PHYSICAL ATTACKS
11 Breaches/Exposures
52,371 Victims

SUPPLY CHAIN ATTACKS
50 Breaches/Exposures
243 Entities Affected
7,510,903 Victims

Top Compromises by Industry in Q1

FINANCIAL SERVICES	*224 Compromises*
HEALTHCARE	*124 Compromises*
PROFESSIONAL SERVICES	*100 Compromises*
MANUFACTURING	*77 Compromises*
GOVERNMENT	*43 Compromises*

Q1 Public Data Breach Notices

550
NOTICES WITHOUT ATTACK VECTOR

291
NOTICES WITH ATTACK VECTOR

Top 5 Compromises by Victim Count in Q1

LOANDEPOT, INC.
16,924,071 VICTIMS

MEDICAL MANAGEMENT RESOURCE GROUP, LLC
2,350,236 VICTIMS

EASTERN RADIOLOGISTS, INC.
886,746 VICTIMS

UNITE HERE
791,273 VICTIMS

PLAZA RADIOLOGY
569,022 VICTIMS

© IDENTITY THEFT RESOURCE CENTER 2024 | IDTHEFTCENTER.ORG

Recent Data Breaches

June 2024

- Truist Bank
- Life360-Tile Data tracker
- Ticketmaster
- CDK Global

May 2024

- JP Morgan Chase
- Dell
- Dropbox
- Ascension Healthcare

April 2024

- US Government-CSO Online Reports
- Giant Tiger
- Roku

March 2024

- Vans
- Fujistu

February2024

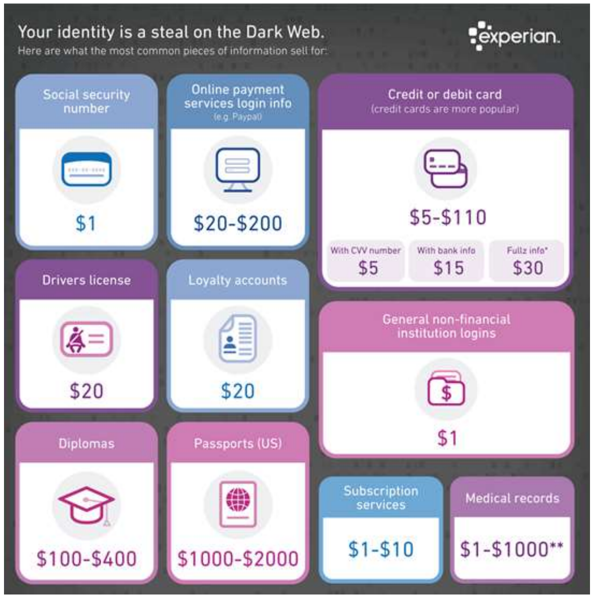
- Bank of America
- Change Health-United Healthcare

January 2024

- Anthropic
- Trello

What’s for Sale

Cyber Attacks on companies and data breaches gather information that was on the systems network and is sold on the dark web.



Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for:

experian.

Social security number
$1

Online payment services login info
(e.g. Paypal)
$20-$200

Credit or debit card
(credit cards are more popular)
$5-$110

With CVV number $5 | With bank info $15 | Fullz info* $30

Drivers license
$20

Loyalty accounts
$20

General non-financial institution logins
$1

Diplomas
$100-$400

Passports (US)
$1000-$2000

Subscription services
$1-$10

Medical records
$1-$1000**

Envisant Achieve your **vision.**

What are Credit Unions' Reporting- Imposter Scams

Scammers initiate contact with a member to obtain access to their private information, accounts, and/or money by impersonating your Credit Union, a trusted professionals, a business or government entity or even a family member.

What are Credit Unions' Reporting-Imposter Scams- *continued*

These scams are successful because of how much legitimate information that can be mined from the dark web. This information enables fraudsters to convincingly impersonate your credit union and have enough information on your members to make it look legitimate.

There is a story..

Crooks hacking into the members accounts.

Stories of credit unions under suspicion and can they help.

Typically, there is a sense of urgency and pressure by the scammer to act. Causing panic so you will act before thinking.

Best Practices for Imposter/Phishing

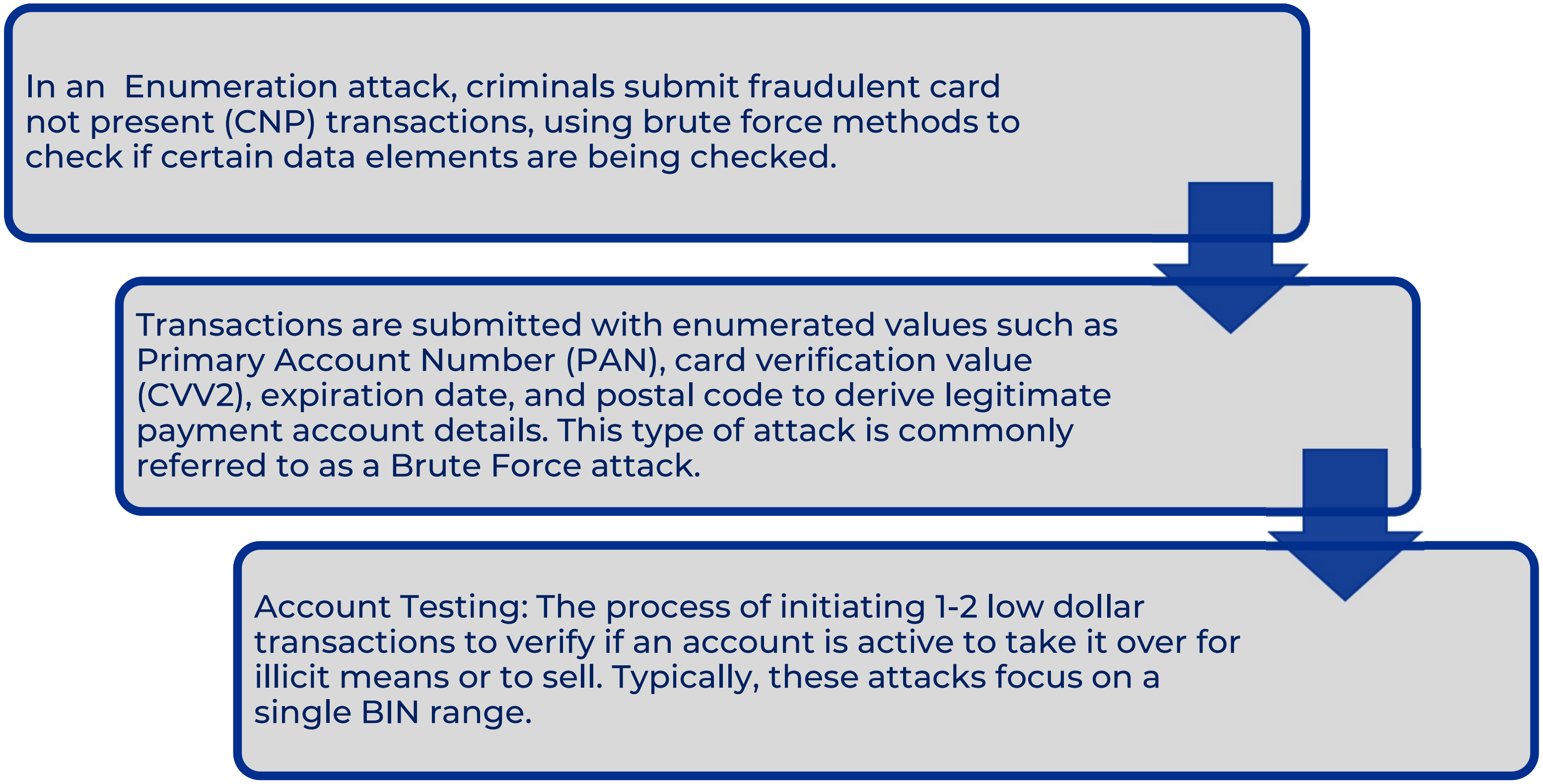
Education for Credit Unions

- Make sure staff knows what is taking place.
- Place a banner on CU's website, phone system, online banking home page of what the CU will never ask for.
- If you use a short code, make sure members know but do not post what it is.
- Let law enforcement know what is taking place.

Education, Education, Education for Members

- Educate Members of the types of fraud and how they take place.
- Members will ***never*** be asked for a full card number, social security number, PINs or two factor authentication codes.
- Online banking credentials should ***never*** be given to anyone.
- If your member is uncomfortable with an automated call, text message or email have them not respond and call the number on the back of their card or the credit union.
- If they are being told not to tell anyone, feel pressured, stop and don't do anything without talking to a trusted family member or friend.

Enumeration and Testing Attacks



In an Enumeration attack, criminals submit fraudulent card not present (CNP) transactions, using brute force methods to check if certain data elements are being checked.

Transactions are submitted with enumerated values such as Primary Account Number (PAN), card verification value (CVV2), expiration date, and postal code to derive legitimate payment account details. This type of attack is commonly referred to as a Brute Force attack.

Account Testing: The process of initiating 1-2 low dollar transactions to verify if an account is active to take it over for illicit means or to sell. Typically, these attacks focus on a single BIN range.

Causes of Enumeration and Testing

The most common method is for fraudsters to target legitimate eCommerce merchants or third-party service providers that have weak fraud controls in place.

Fraudsters can gain access to the payment system by applying for merchant accounts with synthetic merchant identities and use those accounts to conduct enumeration attacks.

Fraudsters perform merchant account take-overs and gain access to the payment system by obtaining a merchant’s login credentials and subsequently taking over their payment gateway to conduct enumeration attacks.

Fraudsters set up cloned point-of-sale (POS) devices or gateways using existing merchant credentials and access processor hosts to submit transactions as part of an enumeration attack.

Due to the lack of fraud controls it makes it hard for the merchant to detect and block fraudulent use of their website for enumeration purposes.·

Criminals target acquirers or agents with weaknesses in their underwriting and onboarding practices that allow fraudsters to open merchant accounts for enumeration attack purposes. •

These credentials can be obtained when a merchant falls victim to phishing schemes, or gateway service providers lack proper merchant authentication when fraudsters call in pretending to be merchants resetting credentials.

This is due to processors who have front-end platform hosts that fail to validate that POS devices or payment gateways belong to their legitimate merchants.

Best Practices for Enumeration and Testing

Utilize	Utilize Card Verification Value (CVV) and CVV2 checking. • Validate accounts, zip code, and expiration dates in all authorization requests. •
Investigate	Investigate authorizations without settlement. •
Monitor	Monitor for spikes on Electronic Commerce indicator (ECI) 06 and ECI 07. •
Alert on	Alert on an increase in reversals being sent.
Block	Block all authorization reversals without original authorizations.
Consider	Consider increasing monitoring and reissuance of accounts involved in both Compromise Account Management System (CAMS) alerts and testing incidents.
Alert on	Alert on BINs with a spike in volume of approvals or declines that would indicate a suspicious event.

Ransomware Attacks

2024 Verizon Data Breach Investigation

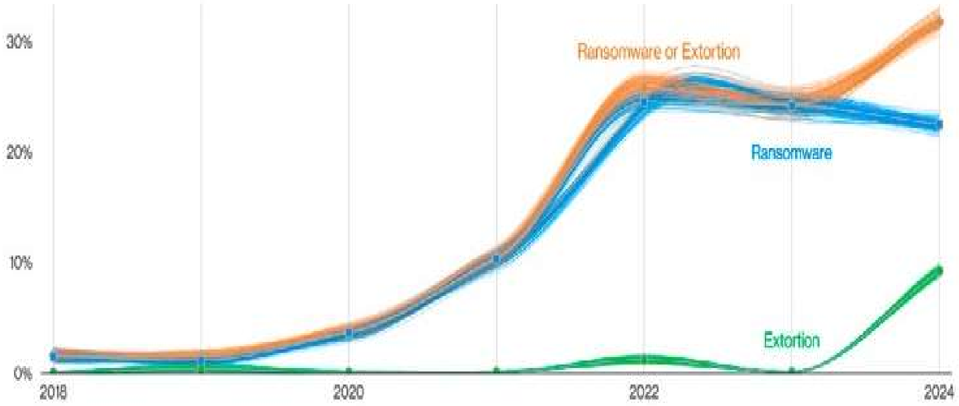


Figure 2. Ransomware and Extortion breaches over time

Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches. The shift of traditional ransomware actors toward these newer techniques resulted in a bit of a decline in Ransomware to 23%. However, when combined, given that they share threat actors, they represent a strong growth to 32% of breaches. Ransomware was a top threat across 92% of industries.

Ransomware Attacks-continued

- Ransomware is malware designed to encrypt files on a device or system that makes them unusable.
- Ransom is demanded to decrypt.
- The fraudsters will threaten to sell or leak the data they have taken.

Best Practices Ransomware

- Employee Training on Phishing Attacks
- Networks are secure and up to date including anti malware and software and firewalls
- ✓ Back up data regularly

Envisant Achieve your **vision.**

Other Common Fraud Trends-Check Fraud

Remote Deposit Capture (RDC)

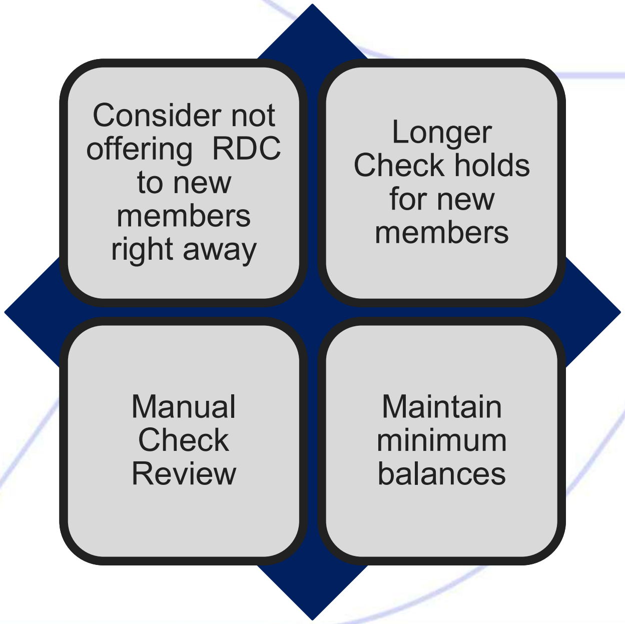
- Account is less than 6 months
- Applied online or in branch
- May have opened more than one account
- Deposit after opening
- Checks are washed or stolen
- Usually larger dollars
- Money leaves account quickly P2P or wire

Other Common Fraud Trends-ATM

ATM Fraud

- ATMs that are not fully EMV enabled
- Skimmer that damages EMV reader
- Transactions are Fallback

Best Practices Common Trends



Consider not offering RDC to new members right away

Longer Check holds for new members

Manual Check Review

Maintain minimum balances

ATM Owner

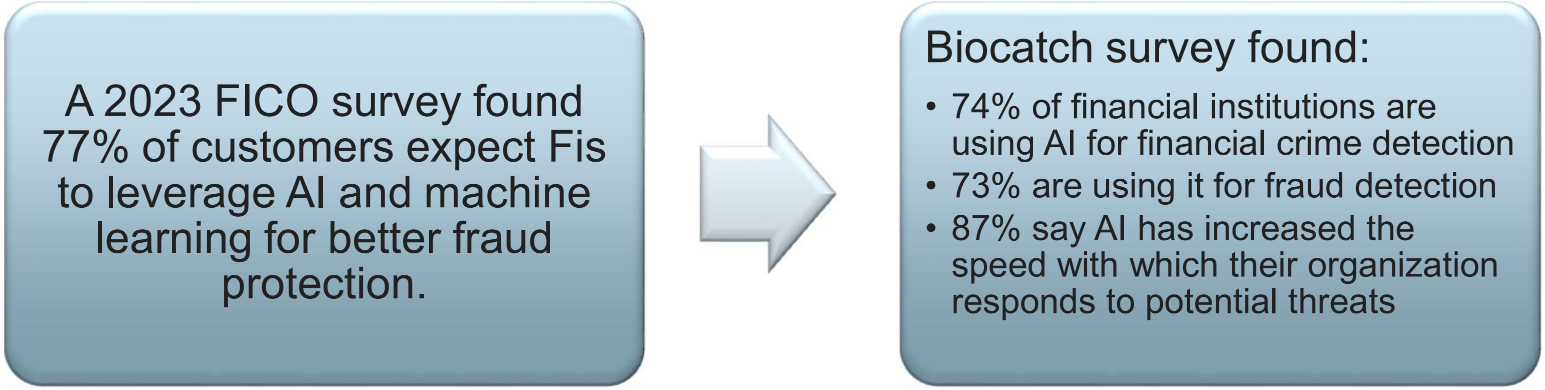
- Make sure all your terminals are enabled for EMV
- Review transactions for fallback
- Investigate Card Reader errors
- Inspect ATM Daily

Card Issuer

- Fallback transaction limits for ATM terminal transactions as well as POS

Artificial Intelligence (AI) and Machine Learning

What is AI?
Technology that enables computers to simulate human thinking or actions. It can be and has been used in many fields for many years. In the financial sector AI in the form of machine learning began in the 1980s



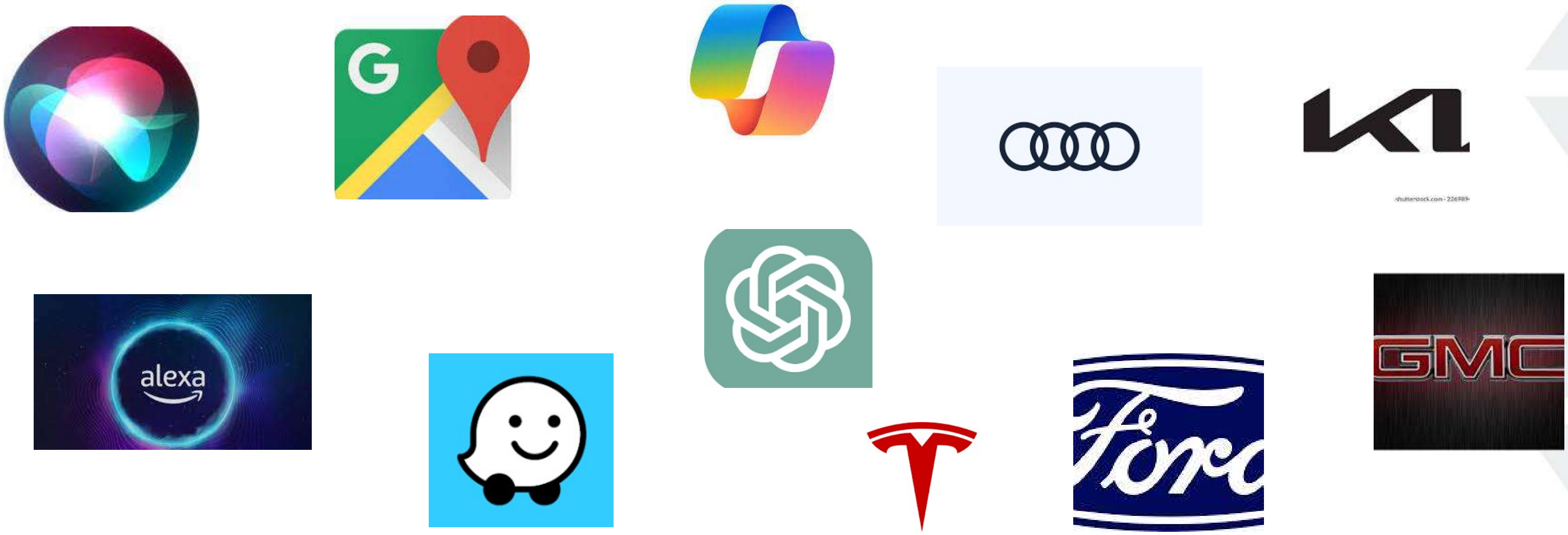
A 2023 FICO survey found 77% of customers expect Fis to leverage AI and machine learning for better fraud protection.

Biocatch survey found:

- 74% of financial institutions are using AI for financial crime detection
- 73% are using it for fraud detection
- 87% say AI has increased the speed with which their organization responds to potential threats

Artificial Intelligence (AI)

Artificial Intelligence (AI) is technology that enables computers and machines to simulate human intelligence and problem-solving capabilities.



Artificial Intelligence (AI)

AI Scams typically are new spins on what we have seen in the past.

Voice Cloning – using social media to find videos or clips of friends and family. May call saying they need money for bail.

Websites- create fake websites with deeply discounted pricing on popular items. Gather PII and payment information.

Video Call Scams- create live fake videos used for video calls.

Phishing Emails- attempts to click on links or downloading malware

How to avoid most scams

Random Calls from friends and family. Look for latency in the speech or pregnant pauses.

Video Scams look for strange shadows or light flickers on the face. Look for abnormal body language.

Emails –formatting may be off from what you would expect. Long formal email.

Questions
Thank You!