TransUnion

EBOOK

Fighting Fraud Across the Account Lifecycle

A playbook for financial services institutions

Financial services institutions (FIs) endeavor to deliver seamless and safe digital experiences, but cybercriminals are relentless, mounting an endless barrage of attacks across the account lifecycle, threatening both customer satisfaction and institutional viability.

Research revealed:

- Identity fraud losses increased by 13% in 2023, amounting to nearly $23 billion[1]
- Account takeover fraud (ATO) alone reached nearly $13 billion, with the incidence rate rising from 67% to 72% (2022 vs. 2023)[2]
- Synthetic identity fraud, the fastest growing type of digital fraud, increased 153% in the first half of 2024[3]
- False positives can cost up to 75 times more than the fraud itself, both in the actual value of canceled transactions and in the opportunity cost of losing further business[4]

Mitigating fraud is especially challenging when the issues are as complex as the solutions. FIs commonly have multiple risk management programs to address varying definitions of fraud throughout the organization. These programs often rely on legacy tools, manual processes and/or third-party vendors to shore up particularly vulnerable access points — but don't necessarily tie to a holistic strategy that covers the entire organization. These siloed programs enhance the risk of cross-channel fraud by hindering effective data management and sharing, creating vulnerabilities by making identity verification difficult.

Despite the challenges, preventing fraud must not come at the expense of the smooth digital experiences today's consumers expect. FIs must effectively balance friction and fluidity or risk losing customers.

What's inside

We created this playbook to help you better understand and navigate the modern fraud landscape. With recommendations and best practices to help you strengthen your current program, this guide shows you how to:

- Discover the underlying key to fraud
- Identify and mitigate the most common fraud types
- Develop a holistic approach that protects the full account lifecycle
- Activate your anti-fraud allies to expand program effectiveness

The underlying key to fraud

Among the various types and scopes of fraud, there's generally one common denominator: **digital consumer identity**. Cybercriminals use stolen consumer credentials and information – gleaned through phishing, social engineering and other tactics – to perpetrate the full range of fraudulent activities.

Core identity credentials are the target of data breaches

In 2024, cybercriminals continued to breach organizations' systems to steal consumer identity credentials required to open fraudulent accounts and create synthetic identities. They also sought credentials like email address, phone number and student ID or school login information to possibly enable account takeover and consumer scams.

The top four exposed identity credentials in US data breaches in the first half of 2024 were:

1. Name
2. Social Security number (full) – exposed in 71% of data breaches
3. Date of birth – exposed in 46% of breaches
4. Home address (current) – exposed in 44% of breaches[5]

Fragmentation creates the greatest risk

With data siloed across internal platforms and/or third-party systems, and no standard, structure or solution to unify them, different parts of the organization have different information about the same person. This fractured view of identity makes it difficult to authenticate good customers and nearly impossible to detect suspicious activities.

Because of this complexity and risk, nearly two-thirds (64%) of US of business leaders surveyed ranked identity verification as the most effective technology for preventing fraud.[6]

If you don't get identity right, everything you do with it will be wrong

From security and compliance to marketing and operations, proper care and handling of consumer identities is integral to business effectiveness. Getting it wrong — using weak or outdated authentication methods, employing outdated data management practices, storing data in isolated silos or not implementing robust security measures, for example — can lead to a broad range of issues, including:

- Fraud and financial loss
- Customer mistrust, dissatisfaction and attrition
- Increased operational costs
- Legal penalties
- Reputational damage

Consistent and accurate verification processes enhance customer experiences by helping to create seamless omnichannel interactions while systematically rooting out bad actors. And when customers trust their transactions are secure, they're more likely to engage with the business, leading to increased loyalty and lifetime value.

Data holds the key to resolving identity

You can address many of the challenges associated with digital identity by focusing on high-quality, well-managed data. The best practices below can help make systems more secure, user-friendly and trustworthy:

- Break down silos with a **holistic data strategy**, establishing identity data linkages across channels
- Help reduce fragmentation and improve consistency across platforms with **universal digital identity management standards**
- Maintain privacy and trust with **user control and consent**, including the ability to manage and revoke permissions
- Enhance security and reduce the risk of identity theft with **strong, multi-factor authentication**
- Increase efficiency with **interoperable systems** that can work seamlessly with each other
- Protect user rights and build trust in digital identity systems by **adhering to regulations** like GDPR and CCPA

Types of fraud and how to fight them

From customer engagement and acquisition to account management and collections, fraudsters are attacking every stage of the account lifecycle. Nearly all parts of the organization are affected and have a stake in combatting it.

Let's explore the four most common types of fraud FIs are confronting today:

- **New account fraud**
- **Credit abuse**
- **Account takeover**
- **Data harvesting**

New account fraud

The most vulnerable stage of the account lifecycle is the beginning — when new relationships are created. New account fraud occurs when a bad actor uses a stolen or fake identity to open a new account and transact as a legitimate customer. Typically used to commit person-to-person (P2P), wire or check fraud, or obtain credit under false pretenses, these accounts increase loss exposure, eroding institutional profitability.

As of the first half of 2024, more than 45% of US financial institutions reported 50%–75+% of their new accounts are created online. As organizations increasingly rely on digital and mobile channels to deliver fast and convenient customer experiences, online new account creation poses increasing risk.[7]

Trends

- 105% global increase in suspected digital fraud occurrences between 2019 and 2023 – outpacing the 90% increase in overall digital transactions[8]
- 18% YoY increase in synthetic identities among newly opened accounts (H1 2024 vs. 2023)[9]
- 37% increase in volume of credit inquiries by potential synthetic identities in 2023[10]

Implications

- **Increased loss exposure:** Estimated outstanding balances for suspected synthetic identities exceeded $3.2 billion, 7% higher YoY and an all-time high[11]
- **Poor digital experiences:** 60% of institutions identified removing friction from consumer authentication as their biggest overall pain point[12]
- **Missed opportunities:** 53% of consumers reported abandoning online applications due to security concerns[13]

How to identify potential new account fraud

If you're experiencing elevated levels of any of the following, you may have an issue with new account fraud and should engage the appropriate resources to address it:

- P2P, wire or check fraud
- Accounts opened with the personally identifiable information (PII) – name, date of birth, passport or Social Security number – of an identity theft victim
- Multiple new accounts using the same phone number, device or IP address
- Suspicious or inconsistent information

Best practices to reduce new account fraud

A view of identity that spans the consumer and their financial and digital behaviors, including on their devices, can enable you to quickly onboard new accounts while minimizing financial and non-financial impacts of new account fraud. Below are best practices for resolving identity and preventing fraud at and after new account origination.

- Prevent high-risk and potentially fraudulent consumers from receiving prescreen offers with fraud models and predictive alternative data
- Resolve both physical and digital elements of an applicant's identity in consumer-initiated prequalification and at account opening
- Assess identity and credit risk at underwriting with trended credit and blended data, fraud models and alerts
- Monitor credit portfolios for evolving credit abuse or bust out risks with data appends and fraud models
- Ensure line increase programs address potential identity risks by including trended credit data and fraud models with exclusion criteria

Deeper dive: Protecting against new account fraud

Learn more about the risks and costs of new account fraud in our blog New Account Creation Fraud and How to Combat It

Discover how a multilayered approach to identity verification at new account opening helps reduce manual reviews while mitigating poor customer experiences and lost sales with Five Steps to Uncover Fraud Before New Accounts Are Opened

Credit abuse

Lenders have more outstanding balances on their books than ever before, with a significant amount of losses attributed to credit abuse. Also known as account abuse, credit abuse is a form of first-party fraud where an individual deliberately misuses their own (legitimate) account or credentials for financial gain. Losses attributed to credit abuse occur in several ways, including P2P, wire or check fraud on deposit accounts, and bust-outs, early defaults or skips on loan accounts. More elaborate first-party fraud schemes include:

- **Money muling**: A type of money laundering where someone transfers or moves illegally acquired money on behalf of someone else
- **Gaming**: Also called promotion abuse, gaming occurs when a consumer transfers balances to take advantage of promotional rates, then defaults on the balances
- **Chargeback fraud**: A consumer uses their card for a purchase, then disputes that purchase with the lender to have the charge removed

Trends

- Consumer credit card balances hit an all-time high in Q1 2024, exceeding $1 trillion[14]
- 9.3% YoY increase in average minimum payment due for prime consumers[15]
- 25% of credit card losses are suspected to be attributed to credit abuse[16]

Implications

- **Increased loss exposure:** Estimated outstanding balances for suspected synthetic identities exceeds $4.6 billion, an all-time high[17]
- **More early defaults:** Early defaults for auto loans, credit cards and personal loans are up between 50% and 90% since 2020[18]
- **Hidden risk:** Despite only accounting for an estimated 0.02% of credit card trades, bust outs account for 11% of card losses[19]

How to identify potential credit abuse

If you're experiencing elevated levels of any of the following, you may have an issue with credit abuse and should engage the appropriate resources to address it:

- Falsified or inconsistent documentation
- Existing accounts that randomly stop paying or stop communicating
- First payment defaults or bust outs on credit cards, auto loans, personal loans
- Rising delinquencies
- Increase in bankruptcy filings
- P2P, wire or check fraud

Best practices to reduce credit abuse

Using models and attributes that pinpoint suspect identities and behavior patterns tied to fraud can help mitigate or prevent losses. Below are best practices to identify and isolate consumers who may be abusing credit or preparing to bust out.

- Prevent high-risk consumers from receiving prescreen offers with fraud models and predictive alternative data
- Identify consumers at higher risk of busting out with payment and fraud models
- Identify higher-risk consumers by integrating identity, credit and device risk tools with new account opening workflows
- Assess credit and malicious behavior risk by using trended credit and blended data, payment and fraud models, and fraud alerts at underwriting
- Monitor for evolving credit abuse or bust our risks by incorporating data appends and fraud models into regular portfolio reviews
- Maintain risk-level line increases by including trended credit data and payment and fraud models in credit line management routines

Deeper dive: The multi-faceted benefits of curbing credit abuse

Learn how empowering consumers with skills to make smart financial decisions can help promote financial inclusion in the blog Empowering Long-Term Financial Well-Being with CARE.

Account takeover

Account takeover (ATO) occurs when fraudsters gain unauthorized access to legitimate consumer accounts or trick account owners into transferring funds out of their accounts. They accomplish this with call and text spoofing, posing as the financial institution or a "person in the middle," and other social engineering techniques to trick a consumer into action. Once an account is taken over, funds are withdrawn, new credit lines are opened or existing ones are maxed out, typically resulting in a total, unrecoverable loss for the institution and an enormous inconvenience — or worse — for customers.

Trends

- 81% increase in global volume of ATO fraud attempts from 2019 to 2022[20]
- 500% YoY increase in reported call spoofing scams (2023 over 2022)[21]
- 29% of consumers reported being a victim of ATO[22]

Implications

- **Increased losses:** Losses from ATO was estimated to be $12 billion in 2022, a 200% YoY increase[23]
- **Reputation risk:** 49% of surveyed consumers ranked the security of their personal data as a top expectation of companies[24]
- **Diminished trust:** 63% of surveyed consumers suggested they would not return to a website if it presented fraud concerns[25]

How to identify potential account takeover fraud

If you're experiencing elevated levels of any of the following, you may have an ATO issue and should engage the appropriate resources to address it:.

- Increases in unauthorized account activity, such as password resets and unauthorized transactions
- Credential stuffing (high velocity login attempts)
- Non-fixed voice over Internet protocol (VOIP) inbound calls to call centers
- Legitimate customers reporting to be victims of scams, including:
  - **Phishing**: fraudulent emails, websites, social posts and QR codes meant to steal data
  - **Smishing**: fraudulent text messages meant to trick people into sharing data or credentials
  - **Vishing**: fraudulent phone calls meant to trick people into sharing data or credentials

Best practices to reduce account takeover fraud

To manage existing accounts against ATO risks, examine risk signals and behaviors in digital and call center channels to intercept higher-risk access attempts while accelerating the process for trusted customers. Outbound call technologies can reduce the risk of customers falling victim to scam calls, while phone risk signals and digital authentication tools decrease the risk of funds transfers when customers unwittingly provide account access. Below are best practices for authenticating consumers and preventing account takeover.

- Secure account access through contact center and online channels by integrating device and consumer identity authentication methods
- Establish and build trust in the phone channel by certifying outbound calls
- Evaluate the risk of inbound call center calls prior to answering a call
- Protect against phone number spoofing with secure one-time password (OTP) for call center and digital channels
- Ensure customer data is up to date by conducting regular data hygiene scrubs
- Accurately resolve identities or locate customers with alternative data, real-time identity verification and skip tracing
- Monitor data breaches and provide consumers with fraud resolution tools as needed

Deeper dive: Protecting against account takeover

By conducting continuous risk assessments, you can authenticate customers without causing undue frustration. Get the insight guide, Mitigate Account Takeover Fraud Through Continuous Risk Evaluation, to learn more.

Data harvesting

Data breaches are a leading indicator of future fraud as cybercriminals are stealing credentials in unprecedented numbers. Data harvesting occurs when fraudsters collect consumer information to build consumer profiles that can be sold and used to commit multiple types of identity fraud. They amass information by conducting web searches, scouring social media platforms and other sites while also attempting to procure data from financial institutions via call center agents, digital banking and even branch channels.

Trends

- 78% increase in the number of reported data breaches in the US in 2023[26]
- 79% of consumers said confidence their personal data will not be compromised is most important when choosing who to transact with online[27]
- 48% of consumers said fraudsters targeted them with fraud attempts in the first half of 2024, with phishing being the most frequent scheme by which they reported being attacked[28]
- 50% of consumers ranked personal data security as the top reason to do business with an online company[29]
- 83% of organizations experienced more than one data breach during 2022[30]

Implications

- **Reputation risk:** 49% of surveyed consumers ranked the security of their personal data as a top expectation of companies[31]
- **Increased operating costs:** In 2022, the average cost of a data breach in the US was $9.4M, including everything from ransom payments and lost revenues to business downtime, remediation, legal fees and audit fees[32]

How to identify potential data harvesting

If you're experiencing elevated levels of any of the following, you may have a data harvesting issue and should engage the appropriate resources to address it:

- Uptick in customer complaints about authentication processes
- Potential inbound call spoofing – inbound caller IDs appearing to be from legitimate customers
- Unusual patterns of data access or requests that trigger alerts
- High-frequency, repetitive transactions
- User suddenly accesses large volumes of data or logs in from multiple locations in a short period of time

Best practices to reduce data harvesting

Inbound authentication minimizes the authentication burden for trusted calls and isolates higher-risk transactions, minimizing the threat of data compromise and social engineering of call center agents. Below are best practices for authenticating inbound contact and preserving consumer trust.

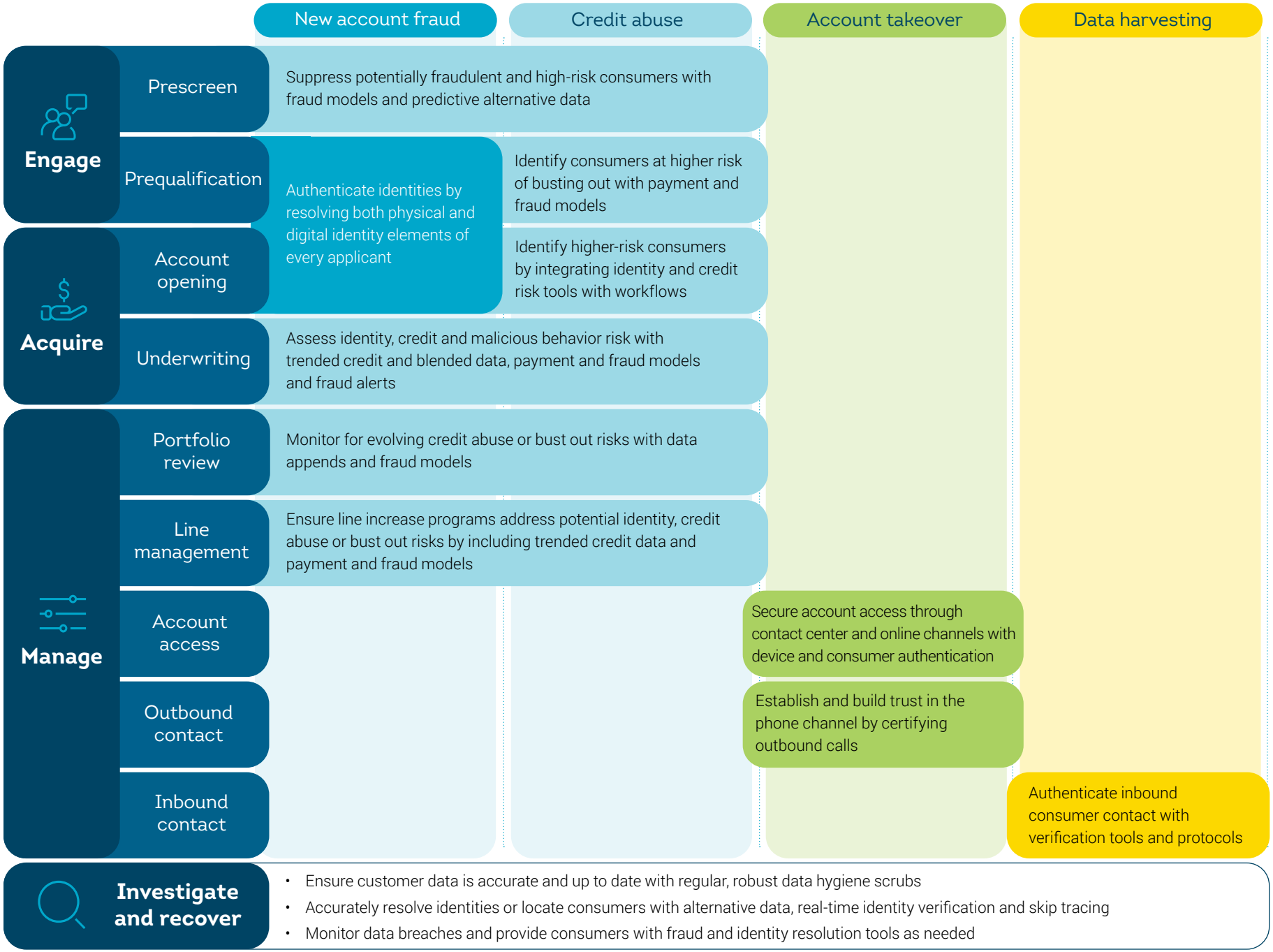
- Authenticate inbound consumer contact by implementing verification tools and protocols
- Accurately resolve identities or locate customers with alternative data, real-time identity verification and skip tracing
- Ensure consumer data is accurate and up to date by conducting regular data hygiene scrubs
- Monitor data breaches and provide consumers with fraud resolution tools as needed

Dive deeper: Get ahead of fraudsters

Stay on top of fraud trends and get important insights on the latest protection strategies in our H2 2024 Update: State of Omnichannel Fraud

Fighting fraud across the account lifecycle

While it's critical to understand and address the specifics of each fraud type, it's also critical to recognize they don't occur in isolation. **A strategic approach to fraud should include a consolidated assessment of institutional risks, implications and opportunities to develop a program that effectively supports the full enterprise by protecting the entire lifecycle**. The matrix below synthesizes the best practices outlined above and can be used as a template to preliminarily assess your current fraud program and create a framework upon which your team can determine next steps.


New account fraud
Credit abuse
Account takeover
Data harvesting
Engage
Prescreen
Suppress potentially fraudulent and high-risk consumers with fraud models and predictive alternative data
Prequalification
Authenticate identities by resolving both physical and digital identity elements of every applicant
Identify consumers at higher risk of busting out with payment and fraud models
Acquire
Account opening
Identify higher-risk consumers by integrating identity and credit risk tools with workflows
Underwriting
Assess identity, credit and malicious behavior risk with trended credit and blended data, payment and fraud models and fraud alerts
Manage
Portfolio review
Monitor for evolving credit abuse or bust out risks with data appends and fraud models
Line management
Ensure line increase programs address potential identity, credit abuse or bust out risks by including trended credit data and payment and fraud models
Account access
Secure account access through contact center and online channels with device and consumer authentication
Outbound contact
Establish and build trust in the phone channel by certifying outbound calls
Inbound contact
Authenticate inbound consumer contact with verification tools and protocols
Investigate and recover
• Ensure customer data is accurate and up to date with regular, robust data hygiene scrubs
• Accurately resolve identities or locate consumers with alternative data, real-time identity verification and skip tracing
• Monitor data breaches and provide consumers with fraud and identity resolution tools as needed

Reinforce your efforts

You're not in this fight alone. Two distinct groups are natural partners in your battle against fraud, and can extend and increase the effectiveness of your program through their own preventative efforts.

Consumers can become powerful anti-fraud allies

Letting consumers know you understand the threats and implications of fraud and are actively taking steps to fight it is a natural way to include them in your quest. **While you have a clear interest in combatting identity fraud, consumers are equally invested in your success.** Their identities are at risk, which is why 59% of surveyed consumers named identity theft as their top cyber concern.[33]

Unfortunately, while converting consumer concern into engagement is an effective strategy that can enhance your anti-fraud efforts, it's often-overlooked. **Consumers want help protecting their credit and identity information**. Half (52%) of those concerned about identity safety haven't tried to improve their situations because they were unsure of what to do.[34]

By educating consumers and offering monitoring solutions that deliver personalized insights and action steps based on their unique situations, you encourage them to be self-sufficient in managing their credit and identities. They can become potent anti-fraud allies who recognize fraud earlier and reduce the risks to them and your financial institution.

Solution providers can keep you at the forefront of fraud mitigation

Working with the right data and fraud prevention provider is essential. One that holistically understands both fraud and consumer identity, specifically within the context of the financial services industry, can provide crucial insights to help you recognize emerging threats earlier and implement the most current solutions to help guard against them.

For more information about strategies and solutions to more effectively fight fraud, contact your TransUnion representative or email:
tu_info@transunion.com

References

[1, 2] 2024 Identity Fraud Study: Resolving the Shattered Identity Crisis, Javelin, April 10, 2024

[3, 5, 6, 7, 9, 11] H1 2024 State of Omnichannel Fraud, TransUnion, October 9, 2024

[4] Deep Dive: How Merchants Can Reduce the Risk of False Positives Through AI and ML, Pyments.com, September 10, 2021

[8, 27, 32] 2024 State of Omnichannel Fraud, TransUnion, May 2, 2024

[10, 12, 13, 15, 16, 17, 20] 2023 State of Omnichannel Fraud, TransUnion, May 3, 2023

[14, 19] TransUnion US consumer credit database

[18] Credit Card and Auto Loan Delinquencies Continue Rising; Notably Among Younger Borrowers, Federal Reserve Bank of NY, February 6, 2024

[21] The Next Critical Phase in the STIR/SHAKEN Fight Against Robocalls: Enterprise Adoption, Forbes.com, October 13, 2022

[22] Account Takeover Incidents are Rising: How to Protect Yourself in 2024, Security.org, September 26, 2024

[23] The Budget and Economic Outlook: 2022 to 2032, Congressional Budget Office (cbo.gov), May 2022

[24, 31] How Americans View Data Privacy: Tech Companies, AI, Regulation, Passwords and Policies, Pew Research Center, October 18, 2023

[25] 86 Percent of Consumers Will Leave a Brand They Trusted After Only Two Poor Customer Experiences, emplifi.io, February 2, 2022

[26, 28, 29] ITRC Annual Data Breach Report, idtheftcenter.org, accessed October 2, 2024

[30] The Devastating Business Impacts of a Cyber Breach, Harvard Business Review (hbr.org), May 4, 2023

[33, 34] Consumer Pulse Q2 2024, TransUnion

TransUnion