ValidiFI®

Detect fraud, in real-time

Validating the identity behind the account.

Ask any banking or payments executive what keeps them up at night, and fraud is likely a top concern. It consumes valuable time, resources, and money.

As attacks evolve at lightning speed, it undermines compliance, damages customer trust, and disrupts business operations.

In this ValidiFI Bank Intelligence Quarterly Report, we share exclusive 2024 bank account fraud insights to help organizations better understand how to detect and stop fraud on the spot.

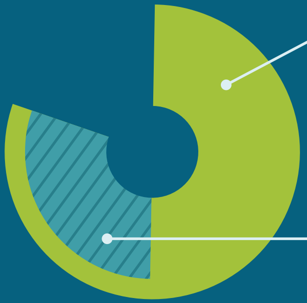
Readers will gain an updated view of fraud and discover:

Surprising fraud elements organizations should be assessing, but many aren't, plus other detailed findings.

How to understand the identity behind an account and tell-tale connections between certain identifiers and fraud.

The power of a layered approach to fraud detection and management that keeps businesses humming, while reducing fraud risk and supporting a stronger bottom line.

Nacha®
Preferred Partner



80% of organizations report being impacted by fraud,

with 30% of those companies failing to recover their fraud losses.

Source: AFPOnline.org

27% of payments executives reported direct losses from fraud exceeding $500,000.

Source: PYMNTS.com

31% of organizations have been forced to modify their internal processes due to fraud incidents.

Source: PYMNTS.com

Identifying multifaceted fraud threats

Manipulating data, altering payment details, and exploiting stolen account information. These are just a few of the convoluted tactics fraudsters use to execute their schemes.

Fraud has become a fast-moving and ever-changing threat in today's digital landscape, putting businesses under immense pressure to protect their payment systems.

Common Types of Fraud:

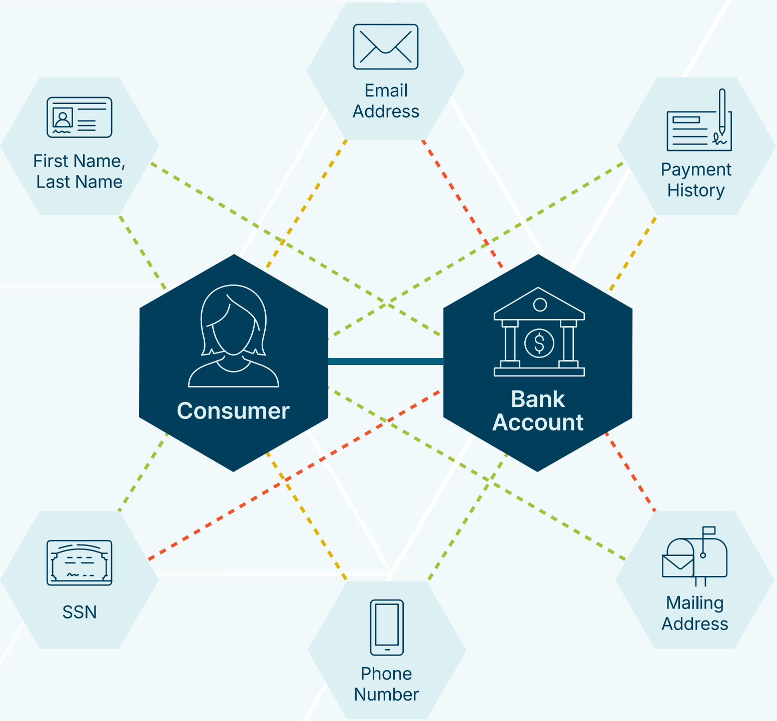
- Synthetic Identity Fraud
- New Account Fraud
- Account Takeover Fraud
- First & Third-Party Fraud
- Application Fraud

This highlights the urgent need for businesses to strengthen their fraud prevention strategies and protect both their assets and their reputation by staying ahead of evolving threats.

So, how can organizations outsmart today's high-tech fraudsters without straining budgets and resources?

The answer lies in data.

Specialized bank account and payment data can uncover hidden patterns, connecting the dots between bank account numbers, routing numbers, SSNs, and other key data elements to expose the larger web of fraud before it disrupts the business.



Let's explore **4 key data elements** organizations should be assessing to strengthen their defenses, according to the Q4 ValidiFI Bank Intelligence analysis.

4 key data elements that can predict fraud risk

1 Phone Number

Fraudsters are **65% more likely to NOT have a verifiable phone number match.**

Consumers with **3+ phone numbers** associated with the same SSN in the last 30 days have a **2.25X greater fraud risk** than average.

Prepaid phones are a higher indicator of fraud. In cases of fraud, 33% were more likely to have a prepaid phone number.

Takeaway:

A few key things to always check associated with a phone number, include:

- Phone carrier type
- Is the number associated with a consumer versus a business?
- Has the phone number previously been associated with other SSNs or bank accounts?

Better understanding these characteristics adds another layer of security to help ensure financial transactions are being conducted by authorized individuals.

2 Email Address

Consumers with **3+ emails** associated with the same SSN in the last 30 days have a **2X times greater fraud risk than average.**

Applications with invalid emails were associated with a **210% increase in fraud rates.**

Emails with a low probability of delivery experienced a **3.3X increase in fraud rates.**

Takeaway:

Identify potential red flags and mitigate fraud risks associated with business email compromise (BEC) vulnerability, by consistently checking:

- Legitimacy of email addresses
- Ability to connect to the email address
- Domain name associated with the email address
- Frequency of email address changes linked to SSNs or bank accounts

BEC fraud is when scammers use fraudulent email tactics to trick employees into sending them money or sensitive information.

Source: 2024 ValidiFI anonymized data study analysis

4 key data elements that can predict fraud risk

3 Name Match

Fraudsters are 60% more likely to NOT have a verifiable first name match.

The likelihood of **fraud increases by 36%** when a last name cannot be matched against verified sources.

Takeaway:

Consumers consistently using the same first and last name pose a lower risk, while frequent mismatches suggest a higher fraud risk.

4 Physical Address

Reported fraud cases **increase at a rate of 130%** when the provided address is not mailable.

When no name or address is reported with the provided phone number, **fraud is 70% more likely** than average.

Fraudsters are **2.3x more likely to have a phone and address zip code mismatch.**

Consumers identified as fraudulent are **62% more likely to list a temporary address.**

Takeaway:

When properly verified, addresses can help reveal fraud. To further strengthen fraud detection, always:

- Confirm an address is valid
- Confirm an address is capable of receiving mail
- Confirm an address is not flagged as suspicious
- Cross-check for consistency with other identity details

Source: 2024 ValidiFI anonymized data study analysis

How ValidiFI data unmasks fraudulent payment accounts

At first glance, some consumers may pass standard account validation checks, showing no signs of fraud. Yet, layering on additional fraud checks can yield deeper insights that reveal critical risk indicators often missed by traditional methods.

For instance, the consumers on the right are real application scenarios from ValidiFI's database, all of whom initially displayed low-risk indicators through a basic account validation.

However, when they were analyzed with ValidiFI's **vFraud** data, their true risk profile became clear, exposing patterns and statistics that unmistakably point to fraudulent activity.

Taking the extra step to automatically cross-reference identity information from application data with bank account-provided details reveals the truth behind the account.

John Doe

- Routing number: **Verified**
- Account number: **Open and ACH capable**
- First name match: **No**
- Last name match: **No**
- # of applications associated with SSN in last 30 days: **23**
- # of bank accounts associated with SSN: **43**

Jane Smith

- Routing number: **Verified**
- Account number: **Open and ACH capable with verified good transaction history**
- # of cleared transactions: **20**
- Address type: **Temporary**
- Bank account and SSN match: **No**
- # of bank accounts associated with SSN: **10**

Robert Brown

- Routing number: **Verified**
- Account number: **Open and ACH capable**
- Phone number: **Unable to verify**
- Phone number type: **Prepaid**
- # of bank accounts associated with SSN: **21**
- # of phone numbers associated with SSN: **17**

This layered approach helps:

Strengthen security by uncovering hidden risks.

Boost confidence in the legitimacy of the account and the individual behind it.

Source: ValidiFI 2024 internal data analysis

Identify telltale connections between key identifiers and fraud

Here are four crucial steps to validate bank account information and ensure that the provided details are legitimate and belong to the applicant.

1 Verify Identity

Performing KYC checks as well as verifying pieces of contact information like phone numbers, email addresses, mailing addresses and whether that information has been seen with a bank account previously, can help ensure you're approving or extending credit to legitimate customers.

2 Validate Bank Accounts

Ensuring fast and accurate bank account validation is critical. Confirming that a bank account is currently valid and active and how long it has been established can reduce errors and ensure financial transactions are processed smoothly, benefiting both the institution and the customer.

3 Assess Connections

This is maybe the most critical step that can uncover hidden or overlooked sophisticated fraud tactics. Cross-checking financial institution data, bank account details, and consumer application data against a third-party database like ValidiFI can help you quickly identify and reject applications with invalid or suspicious information.

4 Fraud Checks

Assessing the above details with known information or patterns of fraud to eliminate the riskiest offenders can help your organization guard against costly incidents. Leveraging predictive data like bank account and payment intelligence, and having a robust validation and bank account authentication process in place are key.

Reduce payment fraud risk with confidence

- **Identify known fraud associations**
- **Detect suspicious indicators**
- **Prevent costly attacks**

CONTACT US TODAY to initiate a complimentary data study and learn how vFraud can empower your organization to outsmart fraudsters.

ValidiFI®

validifi.com