“Should Have Known”: The High Cost of Weak CDD

October 1, 2026

STOUT

Agenda

- Customer Due Diligence Rule
- The 3rd Element of Customer Due Diligence
- The 4th Element of Customer Due Diligence
- Case Studies
- The Impact of Getting It Wrong
- Group Discussion
- Conclusion

The Fifth Pillar of BSA Compliance

Customer Due Diligence Rule

Risk-based CDD is the cornerstone of a strong BSA/AML compliance program, particularly for higher-risk customers

FinCEN identified four core elements of CDD, and mandated that they be explicit requirements in BSA/AML compliance programs for all financial institutions:

1. Customer identification and verification,
2. Beneficial ownership identification and verification,
3. **Understanding** the nature and purpose of customer relationships to develop a customer risk profile, and
4. **Ongoing** monitoring for reporting suspicious transactions and, on a risk-basis, maintaining and updating customer information.

Together, these processes are what let a bank recognize when a transaction is suspicious enough to warrant a SAR

The 3rd Element

Nature and Purpose

The 3rd Element – Nature and Purpose

Understand the nature and purpose of customer relationships to develop a customer risk profile

-The Final CDD Rule, FFIEC Manual, Interagency Guidance on CDD

- Nature and Purpose – Who are your customers and what types of transactions will they conduct
    - At times, nature and purpose can be self-evident, such as for consumer accounts, but certain business accounts may require more information
- Customer Risk Profile - The information gathered about a customer at account opening used to develop a baseline against which customer activity is assessed for suspicious activity reporting.
    - Information can be obtained through customer due diligence questionnaires at onboarding and throughout the customer relationship, but these forms are seldomly updated to address emerging risks
    - *This gap — CDD forms going stale — is exactly what the Customer Risk Rating deep-dive later in this section addresses in detail*

July 6, 2022 - Joint Statement

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Financial Crimes Enforcement Network
National Credit Union Administration
Office of the Comptroller of the Currency

Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence

July 6, 2022

The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Financial Crimes Enforcement Network, the National Credit Union Administration, and the Office of the Comptroller of the Currency (collectively, the Agencies) are issuing this joint statement to remind banks[1] of the risk-based approach to assessing customer relationships and conducting customer due diligence (CDD). This statement does not alter existing Bank Secrecy Act/ Anti-Money Laundering (BSA/AML) legal or regulatory requirements, nor does it establish new supervisory expectations.

The Agencies recognize that it is important for customers engaged in lawful activities to have access to financial services. Therefore, the Agencies are reinforcing a longstanding position that no customer type presents a single level of uniform risk or a particular risk profile related to money laundering, terrorist financing, or other illicit financial activity.

Banks must apply a risk-based approach to CDD, including when developing the risk profiles of their customers.[2] More specifically, banks must adopt appropriate risk-based procedures for conducting ongoing CDD that, among other things, enable banks to: (i) understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile, and (ii) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[3]

Customer relationships present varying levels of money laundering, terrorist financing, and other illicit financial activity risks. The potential risk to a bank depends on the presence or absence of numerous factors, including facts and circumstances specific to the customer relationship. Not all customers of a particular type automatically represent a uniformly higher risk of money laundering, terrorist financing, or other illicit financial activity.

July 6, 2022 - Joint Statement

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation

The Agencies recognize that it is important for customers engaged in lawful activities to have access to financial services. Therefore, the Agencies are reinforcing a longstanding position that no customer type presents a single level of uniform risk or a particular risk profile related to money laundering, terrorist financing, or other illicit financial activity.

Customer type should not be the only factor used to determine customer risk.

Insurance Corporation, the Financial Crimes Enforcement Network, the National Credit Union Administration, and the Office of the Comptroller of the Currency (collectively, the Agencies) are issuing this joint statement to remind banks[1] of the risk-based approach to assessing customer relationships and conducting customer [illegible] (CDD). This statement does not alter existing Bank Secrecy Act/ Anti-Money Laundering (BSA/AML) legal or regulatory requirements, nor does it establish new supervisory expectations.

The Agencies recognize that it is important for customers engaged in lawful activities to have access to financial services. Therefore, the Agencies are reinforcing a longstanding position that no customer type presents a single level of uniform risk or a particular risk profile related to money laundering, terrorist financing, or other illicit financial activity.

Customer relationships present varying levels of money laundering, terrorist financing, and other illicit financial activity risks. The potential risk to a bank depends on the presence or absence of numerous factors, including facts and circumstances specific to the customer relationship. Not all customers of a particular type automatically represent a uniformly higher risk of money laundering, terrorist financing, or other illicit financial activity.

particular type automatically represent a uniformly higher risk of money laundering, terrorist financing, or other illicit financial activity.

Customer Risk Rating Models

- Customer Risk Rating models are often ignored at customization and optimization but their impact on the Suspicious Activity Reporting and Customer Due Diligence requirements is substantial
- Examiners from the Fed, OCC, NCUA, and FDIC have identified Customer Due Diligence as a point of focus in exams and there has been an uptick in CDD failures in consent orders and MRAs specifically concerning:
    - Using inappropriate customer risk scoring methodologies
    - Insufficient higher risk customer reviews
        - Backlogs, Poor Quality, Missing Suspicious Activity

CRR Recap

- Customer Risk Rating (CRR): the individualized assessment of the money laundering/terrorist financing risk posed by a specific customer, distinct from the institution-wide BSA/AML Risk Assessment
- Built from documented factors: customer type, products/services, geography, transaction volume, beneficial ownership, delivery channel
- Assigned through judgmental review, a weighted/automated model, or a hybrid of both
- **Today isn't about building that model. It's about what happens after the rating is assigned, when the file in front of you doesn't match it**

The 4th Element

Ongoing Monitoring and Updating

The 4th Element – Ongoing Monitoring for Suspicious Activity

Ongoing monitoring for reporting suspicious transactions

- Customer Due Diligence (CDD) Final Rule

- "Ongoing Monitoring for reporting suspicious transactions" – when a customer engages in transactions that are not of the sort the customer would normally be expected to engage, CDD (among other sources) is one means of determining whether the activity is suspicious

- CDD only earns its value here — a risk profile that is never compared against actual account activity is paperwork, not a control

- A monitoring alert without an accurate customer profile behind it is guesswork — the profile is what turns an unusual transaction into a suspicious one

The 4th Element – Ongoing Monitoring for Suspicious Activity

On a risk-basis, maintaining and updating customer information

- Customer Due Diligence (CDD) Final Rule

- CDD should be updated based upon particular events, such as changes in expected activity
  - "This provision does not impose a categorical requirement that financial institutions must update customer information…on a continuous or periodic basis. Rather, the updating requirement is event-driven, and occurs as a result of normal monitoring." – Final Rule
- The same event-driven logic applies to a customer's risk rating — new products or geographies, ownership changes, adverse media, or a material change in transaction volume or pattern
- Treating CDD as fixed at onboarding is exactly the gap that let Canaccord's customer files go stale for years

Case Studies

CASE STUDY

Canaccord Genuity LLC

- **March 2026:** FinCEN assessed an $80 million civil money penalty against a broker-dealer, the largest ever imposed on a broker-dealer for BSA violations
- **Root cause:** the firm rated risk at the account-type level rather than the individual customer level, so it never built a process for individualized CDD
- **Result:** higher-risk applicants received the same level of due diligence as lower-risk applicants, because the model never distinguished between them
- **Downstream effect:** missed connections to sanctioned individuals, and at least 160 suspicious activity reports never filed (lookback)
- **Takeaway:** getting the unit of analysis wrong undermines everything built on top of it — EDD, monitoring, and SAR decisions all inherit the same blind spot
- ***Looking ahead:*** *ties directly to Missing or Late SARs as a Red Flag*

CASE STUDY

Community Federal Savings Bank

- **April 2026:** the OCC issued a consent order against Community Federal Savings Bank, a single-branch bank that grew from under $140 million in assets (2017) to nearly $900 million (2024), almost entirely through fintech and payments partnerships
- **Root cause:** the bank's CDD program was "ineffective" because it did not understand the nature of certain customers' businesses or the purpose of their transactions
- **Calibration gap:** its automated alerting system had filtering thresholds that were never tuned to its payment-processing risk profile, so its triage logic auto-closed a very high percentage of alerts that should have been escalated
- **Takeaway:** a CDD program can't apply risk-based scrutiny it doesn't understand it needs — the bank's growth outpaced its ability to actually know its own customers
- ***Looking ahead:*** *this calibration gap is exactly what Adjusting the Risk Rating — Closing the Loop is built to prevent*

The Impact of Getting It Wrong

The Cost of Getting It Wrong

- The regulatory escalation ladder rarely skips steps:
  - 1. Matter Requiring Attention (MRA) or Matter Requiring Board Attention (MRBA)
  - 2. Formal enforcement action, consent order or written agreement
  - 3. Civil money penalty
  - 4. Lookback review, often with a SAR refiling requirement covering the affected period
- A lookback isn't a one-time cost. It means reopening every file the flawed rating touched, sometimes years of them
- The trigger for escalation is almost always the same at every step: examiners found something the institution should have caught first

“Should Have Known” — Exposure Beyond BSA

- BSA/AML enforcement isn’t the only exposure. Weak CDD can pull an institution into:
  - Criminal investigations, even when the institution had no intent to facilitate wrongdoing
  - Grand jury subpoenas for account records and internal communications
  - Civil litigation from victims of fraud or laundering schemes conducted through the account
- The legal standard that matters here isn’t “did the institution know.” It’s “should the institution have known”
- *A documented, applied, and actually-followed CDD program is the best evidence an institution has that it met that standard. An undocumented one is evidence of the opposite*

Missing or Late SARs as a Red Flag

- To examiners and law enforcement, a pattern of late, incomplete, or missing SARs isn't a paperwork problem. It's a signal that the underlying risk identification failed somewhere upstream
- Common upstream causes:
  - A risk rating too low to trigger the review that would have caught the activity
  - Alerts closed without adequate documentation of why
  - Backlogs that push filings past the 30-day (or 60-day, with suspect identification pending) deadline
- A SAR backlog audit often traces back to the same handful of customer risk ratings, not a random distribution across the portfolio

When to Challenge Customer-Provided Information

- Red flags that warrant a follow-up question, not just a filed form:
  - Stated occupation or business type doesn't match the transaction pattern
  - Business description is generic enough to apply to almost any company ("consulting," "import/export," "trading")
  - An explanation that answers a different question than the one asked
  - Documentation that's facially valid but unverifiable (a business license for an address that's a residence, a website with no operating history)
- The test isn't "is this answer plausible." It's "does this answer hold up if I ask one more question"
- Recording an implausible answer without follow-up is worse than not asking at all. It creates a file that looks diligent but wasn't

When to Escalate

- Escalation triggers, at minimum:
  - Customer explanation doesn't survive a follow-up question
  - Activity is materially inconsistent with the stated business or the current risk rating
  - Adverse media, law enforcement inquiry, or subpoena touches the account
  - Front-line staff has a documented, unresolved concern after normal review
- The pathway should be defined before someone needs it: line staff to BSA Officer or designated escalation point, then to an EDD or SAR committee if warranted
- "Don't sit on it" is a timing standard, not a slogan. Build an expected turnaround for each escalation tier and track exceptions

Adjusting the Risk Rating — Closing the Loop

- Learning something new about a customer isn't the end of the process. The rating has to actually move, and that requires:
  - Documenting what changed and why the rating moved (or why it didn't, after review)
  - Re-running EDD if the customer moves into a higher tier, not just noting the new tier
  - Confirming the updated rating actually reaches the monitoring rules and alert thresholds that key off it
- A rating that changes in one system but not the other isn't an adjustment. It's a data entry exercise
- This is the same event-driven logic from the 4th Element: new products, ownership changes, adverse media, or a material change in volume or pattern

Validation and Periodic Re-Tuning

- A customer's risk rating at onboarding is a snapshot, not a lifetime designation
- Independent testing should evaluate the CRR *model*, not just whether staff applied it correctly
- Common re-rating triggers:
  - New products, services, or geographies added to the relationship
  - Ownership or control changes
  - Adverse media or law enforcement inquiries
  - Material change in transaction volume or pattern
- **Review cadence** should itself be risk-based: higher-risk customers reviewed more frequently than lower-risk ones

A Shifting Regulatory Posture

- **Pattern:** regulators are now naming CRR methodology as a specific, standalone finding, not folding it into a generic "CDD is weak" conclusion
- **April 2026 FinCEN NPRM:** proposes giving institutions more explicit discretion to direct resources toward higher-risk customers and activities
  - Separates establishment from implementation — enforcement is reserved for establishment failures or significant, systemic gaps, not minor technical ones
  - Directs institutions to put more resources toward higher-risk customers and less toward lower-risk ones — the differentiation a flat CRR can't act on
- **November 2025 OCC bulletin:** gives examiners room to scale testing based on an institution's actual risk profile, rather than applying uniform expectations across all community banks
  - Lets examiners rely on a bank's own satisfactory independent testing of its CDD/CRR program instead of duplicating it — the exact reliance Community Federal Savings Bank's weak testing couldn't earn
- **Net effect:** a well-built, well-documented CRR isn't a checkbox anymore — it's becoming the mechanism regulators expect institutions to lean on

Group Discussion

DISCUSSION

Scenarios — Challenge, Escalate, or Accept?

- Scenario 1: A retail business customer whose wire activity over the past two quarters shows recurring international transfers to a jurisdiction never mentioned at onboarding, with no site visit or follow-up on file

- Scenario 2: An individual customer with expected annual income of approximately $100,000 and primarily domestic account activity has, over the past six months, received multiple incoming international wires totaling more than $400,000. When asked about the activity, the customer states that the funds are related to “personal investments and money from family.”

- Scenario 3: A restaurant customer with expected account activity consisting primarily of credit card receipts, checks, and electronic payments has, over the past several months, made increasingly frequent cash deposits totaling approximately $150,000. When asked about the increase in cash activity, the customer states that more customers are choosing to pay in cash to avoid credit card processing fees.

Conclusion

Conclusion

- Regulations are all about intent and the intent of the CDD rule is to ensure that FIs know their customers
- **Customer Risk Rating** is what makes the rest of this list risk-based instead of uniform — without a well-built CRR, EDD, monitoring, and updates default to the same treatment for every customer
- At onboarding:
  - No customer type presents a single level of uniform risk — Canaccord and Community Federal Savings Bank got there in two different ways
  - Unclear or unusual CDD should be clarified
  - Higher Risk ≠ High Risk — a customer can land in an elevated CRR tier without automatically requiring full high-risk treatment
  - EDD is additional information obtained to better understand the nature and purpose of the customer relationship
- Ongoing Monitoring:
  - As needed, update CDD to ensure that the information is accurate and helpful
  - Don't try to explain away unusual activity
  - Update your CDD forms/questions to account for new risk
- When it breaks down:
  - Missed or late SARs, and CRR/EDD failures, are what turn into consent orders and MRAs
  - Challenge inconsistent answers and escalate before accepting an explanation that doesn't hold up
  - When a rating changes, close the loop — document it, re-run EDD, and confirm monitoring rules pick up the new tier

Questions?