CIP and identity

EY
Building a better working world

You satisfied CIP collection and documentation requirements. But did you onboard a criminal?

Traditional CIP controls at onboarding effectively meet current collection and documentation requirements but do not fully verify customers' identity or protect your financial institution from the risk of onboarding criminals. How can your financial institution verify that a customer's claimed identity in fact matches their actual identity? The increasing sophistication of criminals enabled through fraud-as-a-service (FaaS), where a criminal supplies tools and services to other criminals to facilitate their commission of fraudulent online activity; the proliferation of synthetic identities; and easy access to personally identifiable information (PII) within the public domain is diminishing the ability of financial institutions to rely on traditional collection and verification practices.

The Customer Identification Program (CIP), as defined by the United States Department of the Treasury USA PATRIOT Act of 2001 – 31 C.F.R. § 103.121, requires financial institutions to implement reasonable procedures to verify the identity of a person seeking to open an account. Criminals are increasingly circumventing traditional, sometimes highly manual, CIP controls, leaving financial institution executives asking: "We are satisfying CIP requirements, but how do I know if an identity has truly been verified?"

Combating onboarding CIP and fraud risks in brief

- Seek to strengthen their CIP program at onboarding by leveraging identity proofing solutions to verify a customer's claimed identity. This includes alignment of onboarding and identify verification functions and controls across financial crimes.
- Define a target-state identity and verification model that utilizes a multipronged detection strategy. This includes designing an identity system architecture and capabilities utilizing identity proofing to increase efficiency, effectiveness, emerging CIP and fraud risks.
- Design a target-state implementation plan and secure resources to execute against it.

Evolving identity verification and authentication landscape

Increased demand for frictionless, simpler and more secure customer experiences has contributed to the rapid digitization of customer onboarding at financial institutions. This is evidenced by the online channel accounting for 48% of credit card application submissions while only 29% of applications are submitted at branch locations. For traditional checking accounts, 42% of applications are submitted at branches and the online channel represents 37% of checking account applications.[1] This rapid migration of customers seeking the ease of the online channel, record-breaking data breaches and the proliferation of synthetic identities has created a perfect storm for criminals to circumvent the current and manual CIP collection and verification controls deployed by financial institutions.

Data breaches

The top 50 data breaches between 2004 and 2021 led to 17.2b data records leaking online, accessible to a global audience of criminals.[2] Criminals leverage this data in a multitude of ways, including submitting fraudulent credit card applications, applying for fraudulent loans, launching account takeovers, filing fraudulent insurance claims and producing synthetic identities.

Identity theft

PII is increasingly becoming accessible in the public domain of information, resulting in an increase in identity theft. Nearly 42m Americans were victims of identity fraud in 2021, costing consumers $52b in total losses, according to a new report cosponsored by AARP.[3]

Synthetic identities

Synthetic identities are a combination of fabricated PII that is not associated with a real person. Synthetic identities may be created using potentially valid PII, such as a Social Security number or tax ID, accompanied by other fictitious indicators to give the appearance of a true identity. Synthetic identities have been plaguing credit card and lending institutions for several years, with conservative estimates attributing synthetic identity fraud for unsecured US credit products totaling US$1.8b in 2020 and estimated to grow to US$2.94b in 2025.[4] In recent years, criminals have expanded the utilization scope of synthetic identities to fraudulently opening demand deposit account (DDA) and small business accounts. By successfully opening DDAs with synthetic identities, the criminal is given a degree of validation, while the attacks on small business accounts are designed to secure the larger lines of credit associated with these accounts.

Deterioration of customer trust

As customers continue to be victimized by identity theft, account takeovers and other instances of fraud, customer trust in traditional financial institutions has begun to erode. Eighty-seven percent of Americans said that it is very or extremely important that they trust a company to verify their identity effectively and smoothly during a new account opening experience.[5] Additionally, over 50% of Americans indicated that they would not do business with a company in the future if an unauthorized account was opened in their name at that business.[5] As financial institutions square off in the ultra-competitive landscape of customer acquisition and loyalty, they must factor in the impact of the efficiency and effectiveness of their identity verification at onboarding.

Regulatory risk

These risks are not going unnoticed by regulators. Signaled by the passing of the Anti-Money Laundering Act 2020 (AMLA), financial institutions are required to modernize their Bank Secrecy Act (BSA)/anti-money laundering (AML) program and strengthen their identity verification capabilities to comply with updated beneficial owner and politically exposed person (PEP) requirements. Additionally, the Federal Deposit Insurance Corporation (FDIC) and Financial Crimes Enforcement Network (FinCEN) collaborated to launch the "FDIC FinCEN Digital Identity Tech Sprint" aimed at identifying solutions that would increase operational efficiency and account security, reducing fraud and identity-related crimes, money laundering and terrorist financing, and foster customer confidence in the digital banking environment.[6]

[1] Conroy, Julie, "Application Fraud: How Do You Solve a Problem Like Identity?" *Aite-Novarica website* (https://aite-novarica.com/report/application-fraud-how-do-you-solve-problem-identity), December 6, 2022.

[2] Brooks, Chuck, "Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know," *Forbes website* (https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=72adf3867864), June 3, 2022.

[3] Terrell, Kenneth, "Identity Fraud Hit 42m People in 2021," *AARP website* (https://www.aarp.org/money/scams-fraud/info-2022/javelin-report.html), April 7, 2022.

[4] Conroy, Julie, "Synthetic Identity Fraud: Solution Providers Shining Light Into the Darkness," *Datos Insights website* (https://aite-novarica.com/report/synthetic-identity-fraud-solution-providers-shining-light-darkness), June 14, 2022.

[5] IDology, "Inside the Mind of the Insecure, COVID-Weary Consumer," Fourth Annual Consumer Digital Identity Study (preprint), 2021.

[6] "FDIC and FinCEN Launch Digital Identity Tech Sprint," *FDIC website* (fdic.gov/news/financial-institution-letters/2022/fil22004.html), January 11, 2021.

Staying ahead of the threat through identity proofing and implementing effective CIP

Financial institutions should seek to strengthen their CIP program at onboarding by leveraging identity-proofing solutions to verify a customer's claimed identity. Identity proofing encompasses a single, complete customer identity which connects identity attributes such as behavior and device information and compares that information against internal and external sources to detect anomalies. Deploying an identity-proofing strategy using multiple data attributes, such as identity based on life history (credit report) and biometrics (facial scan), enables financial institutions to integrate customer identification and verification controls throughout the customer journey, unlocking better customer experiences by securely reducing friction and lowering the cost of controls. Information provided by customers at enrollment is used throughout the customer lifecycle and compared against internal and external data sources, and their identity is proofed at each interaction, or transaction. Identity proofing consists of integrated and orchestrated authentication enabling standard control capabilities across all channels and provides a more consistent customer experience. While financial institutions are largely already employing varying degrees of identity-proofing solutions for fraud prevention, taking a transformative approach to customer identity focused on orchestration and integration will drive consistency in mitigating customer identity risk.

To begin this effort, financial institutions should take the following steps:

1. Perform a rapid assessment of existing identification and verification controls (people, process and technology) across know-your-customer (KYC), fraud and cyber against both today's threats and emerging threats and the strategic growth of the firm:
    a. Evaluate the inherent risk and control environment effectiveness against the financial institution's desired customer experience objectives and risk appetite.
    b. Evaluate the current technology architecture and capabilities to identify where a full replacement or supplement to current capabilities is needed to address CIP and fraud onboarding risk. Dynamic technology capabilities are required to mitigate new CIP/fraud threats and accompany overall firm growth.
    c. Evaluate activities performed during the onboarding process identifying redundancies across CIP and fraud teams performing similar identification and verification processes utilizing the same data elements.
2. Leveraging the rapid assessment results, define a target-state identity and verification model that utilizes a multipronged detection strategy.
    a. Establish an anti-financial crime identity solution architecture that uses a variety of detection signals that can profile the digital identity of the application submission and provide insight on whether an identity is genuine or synthetic.
    b. Establish a right-sized onboarding identity and authentication framework. This framework should define policies synchronized with risk tolerance and provide clear traceability from policies to detailed controls and procedures.
3. Design a target-state implementation plan and secure resources to execute against it. This includes establishing an ongoing change management plan which challenges your operating model and identity framework on an ongoing basis against emerging threats, your institution's risk appetite and evolving regulatory expectations.

This improved standardization of identity and verification practices, policies and technology solutions across onboarding functions can improve operational efficiency and reduce cost through addressing redundancies in operational practices and cross-utilization of technology. Customer friction will be reduced while better protecting the financial institution against criminals. As financial institution executives lead their institutions away from traditional collection and verification practices used for CIP and towards a more bank-wide identity proofing approach, they will achieve an increased level of confidence that a customer's identity has truly been verified.

Identity proofing across the customer lifecycle

Top-tier US financial institution

Client challenge

Our client was experiencing over USD$10m in losses due to wires monthly. The institution's customer base has seen rapid growth, and the current technologies using manual identity verification have increased costs and lack the ability to scale with the base. Specifically, the existing wire process was inefficient, insecure and prone to fraud, leading to poor customer experience.

Solution

We performed an assessment of existing controls across people, process, and technology. Defined and implemented a solution that leveraged orchestration and mobile first approach that improved the customer experience for wires and reduced fraud losses. Prioritizing the mobile channel as the primary way of interacting with customers and delivering services.

Key issues

- Insecure initiation leading to high rates of compromise. Wire could only be initiated through email or the banker.
- High friction and delayed execution resulting in poor customer experience. All wires required a client callback for execution.
- Manual and inconsistent authentication controls that could easily be manipulated. The customer's identity was confirmed by the banker recognizing the customer's voice.
- Inefficient technology architecture and operating model creating confusion and increased costs. Several independent monitoring systems generated alerts for separate groups throughout the institution.

Value delivered

- Implement orchestration sequencing controls based on risk of the signals in the transaction.
- Identity proofing and risk-based authentication when risk exceeds thresholds defined by institution's risk appetite.
- Move to mobile-first to enable customers to initiate and approve wires securely through their mobile devices.
- Develop a centralized fraud data hub for better cross-channel monitoring.

Benefits

- Reduced fraud losses by over 80%, saving the bank more than USD$8m per month.
- Improved customer experience by reducing call-backs, delays and friction in the wire process.
- Enhanced security by verifying customer identity with biometric and liveliness checks, device binding and out-of-band questions.
- Increased efficiency by streamlining and automating the wire process with orchestration and mobile-first.

Ernst & Young LLP team and services

Our global Financial Crimes Compliance team has worked with several financial institutions to support CIP and fraud identity program enhancements. This support ranges from tactical process and technology enhancements to defining their target-state identity strategy, designing identity system architecture and serving as the multiyear transformation advisor.

We are an industry leader in providing anti-fraud, anti-money laundering, sanctions compliance risk and technology advisory services to financial institutions, financial technology firms and other industries. To learn more about our experience, please reach out to any of the following subject-matter advisors:

Rob Mara
Financial Crimes Compliance
Ernst & Young LLP, Principal
robert.mara@ey.com

Kristin Gilkes
Financial Crimes Compliance
Ernst & Young LLP, Principal
kristin.m.gilkes@ey.com

Amanda Schweizer
Financial Crimes Compliance
Ernst & Young LLP, Senior Manager
amanda.m.schweizer@ey.com

Joseph Getty
Financial Crimes Compliance
Ernst & Young LLP, Manager
joe.getty@ey.com

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

2309-4338969
ED None
22197-241US

ey.com