Bottomline

How Payments Hubs Help You Stay **Competitive** and **Compliant**

NACHA 2026 CHANGES SHED LIGHT ON PAYMENTS HUB BENEFITS

bottomline.com

1 Introduction

Mounting threats of payments fraud and increased regulatory pressure are adding layers of concern and administration work for treasury teams. Whether it's preemptively adding safeguards to protect financial data or keeping tabs on all the new and existing compliance regulations, the workload and worry are not going away. For example, implementing the upcoming rule changes from Nacha—the organization that ensures secure, efficient, and standardized electronic payments for consumers and businesses—will add additional steps to the ACH payments process. It's a lot to manage.

On a parallel path and with similar urgency, payment volumes are surging for treasury and payment teams, while payees expect accurate, secure, and speedy payouts. For many organizations, payments systems that have worked in the past have become a liability. Non-automated and frustratingly fragmented, these antiquated systems and processes have created blind spots and increased exposure to fraud and compliance errors.

At stake are expensive penalties, disappointed payees, and unpredictable financial losses. Businesses are asking if there is a better path forward.

What's the best solution?

A secure, automated payments solution, such as a Payments Hub, can help mitigate these growing concerns. A Payments Hub centralizes payment orchestration and provides clear visibility into payments. It saves time and effort for treasury professionals and accounts payable teams by providing user-friendly workflows, payments approvals, and detailed reporting.

Furthermore, with a Payments Hub, organizations can **shift** from a reactive risk management mindset to a strategic and proactive mindset.

Payments Hub users save considerable time and money with security and compliance features built-in to the solution. Audits are automated. Compliance and fraud controls are layered into every transaction. Treasury teams get to adapt to new regulations without sacrificing speed or security.

Those that choose to modernize with a Payments Hub sever the slow ties of legacy systems and unlock efficiencies that drive long-term growth. For these reasons and more, it's time for future-focused organizations and leaders to select and leverage a comprehensive Payments Hub.

2 Payments Pressures: Fraud Risks, Compliance Deadlines, and High Expectations for Today's Treasury Teams

Payment operations are under increasing strain, driven by surging transaction volumes and evolving customer expectations for accuracy, speed, and security. Legacy systems, often non-automated and fragmented, have become liabilities. These outdated infrastructures create operational blind spots and increase the risk of both fraud and compliance failures.

According to the 2025 AFP® Payments Fraud and Control Survey, 79% of organizations experienced payments fraud attacks or attempts in 2024. In fact, the most prevalent and damaging forms of ACH credit fraud—vendor impersonation and business email compromise (or BEC)—continue to exploit gaps in payment workflows and approval processes today.

Compounding these challenges are the upcoming 2026 Nacha rule changes, which are among the most impactful regulatory shifts in the past two decades. Depending on annual ACH transaction volumes, businesses must implement risk-based fraud detection and monitoring systems within the next few months. The urgency of these regulatory expectations highlights the critical need for dynamic solutions capable of combating sophisticated fraud threats.

Consequently, organizations are looking for a way to manage payments effectively in an environment shaped by regulatory complexity, operational vulnerabilities, and shifting market expectations. They need a modern, strategic approach to payments and risk management

Fragmented Controls

Centralized Controls

Business Payments Face Pressures from Multiple Sides

REGULATORY COMPLEXITY:

Organizations must navigate a patchwork of requirements across multiple jurisdictions, including anti-money laundering (AML), Know Your Customer (KYC), sanctions, and data privacy. This complexity demands consistent, provable controls throughout every payment transaction.

OPERATIONAL VULNERABILITIES:

Point solutions and customized integrations introduce blind spots, inconsistent policies, and higher error rates, ultimately increasing organizational risk.

MARKET DYNAMICS:

Customers increasingly expect real-time, transparent, and resilient financial experiences. Satisfying these expectations requires robust orchestration and observability within payment infrastructures.

Recent Compliance Changes Effecting Business Payments

Nacha:

The National Automated Clearing House Associationis implementing significant rule changes beginning in 2026. To improve security and clarity in transactions, Nacha changes include:

1. Mandatory Risk-Based Fraud Detection

- Organizations processing ACH transactions must implement risk-based fraud detection systems. Specific deadlines are dependent on ACH transaction volumes.
- Businesses will need to establish processes to identify suspicious transactions, review fraud detection measures, and train staff to recognize warning signs, such as sudden changes in vendor payment details.

2. Standardized Payment Descriptions

- ACH transactions will require specific terms for payment descriptions. Changes are meant to enhance clarity and assist in fraud monitoring.
- Organizations will need to update their accounting or ERP systems to comply with new formatting rules.

3. Implementation Guidance

- Businesses are encouraged to prepare now by reviewing ACH transaction volumes, updating internal controls, and documenting fraud prevention steps. Having regular reviews of payment template standardization is also recommended.
- To gain insights and tools for compliance, Nacha recommends consulting with financial partners.

ISO 20022:

An international standard for electronic data exchange between financial institutions, ISO 20022 defines a common language and data format for financial messages so banks, payment systems, and markets can communicate more clearly and consistently.

For North America, ISO 20022 migration is now the operating standard. Banks and payment infrastructures have fully transitioned, making ISO-ready data, formats, and controls essential for efficient, compliant, and cost-effective payment operations. Although corporates are not directly regulated to a single deadline, some banks are starting to request that they migrate their integrations too.

3

The Basics: How Using a Payments Hub Helps Businesses Move Money

A Payments Hub connects and centralizes payment orchestration, transforms multiple payment types and formats, controls various processing needs, and secures payments with compliant-friendly sanction screenings and authentication measures.

Using cloud-based technology, Payments Hubs help companies centralize and automate multiple payment types such as wire, international, and ACH transactions. The technology simplifies bank account verification, payment transaction approvals, fraud prevention, and more. With intuitive features and integration with existing financial systems, a robust Payments Hub can transform payments into a core competency. This kind of solution can replace manual, time-consuming, and error-prone processes with real-time accuracy and control.

From orchestrating payment flows across channels and geographies to expertly embedding compliance and risk controls, Payments Hubs let businesses get more done.

Here's a run-down of other core capabilities of this type of solution:

CONNECTIVITY:

Payments Hubs connect banks, networks, rails, and gateways using standard APIs.

ORCHESTRATION:

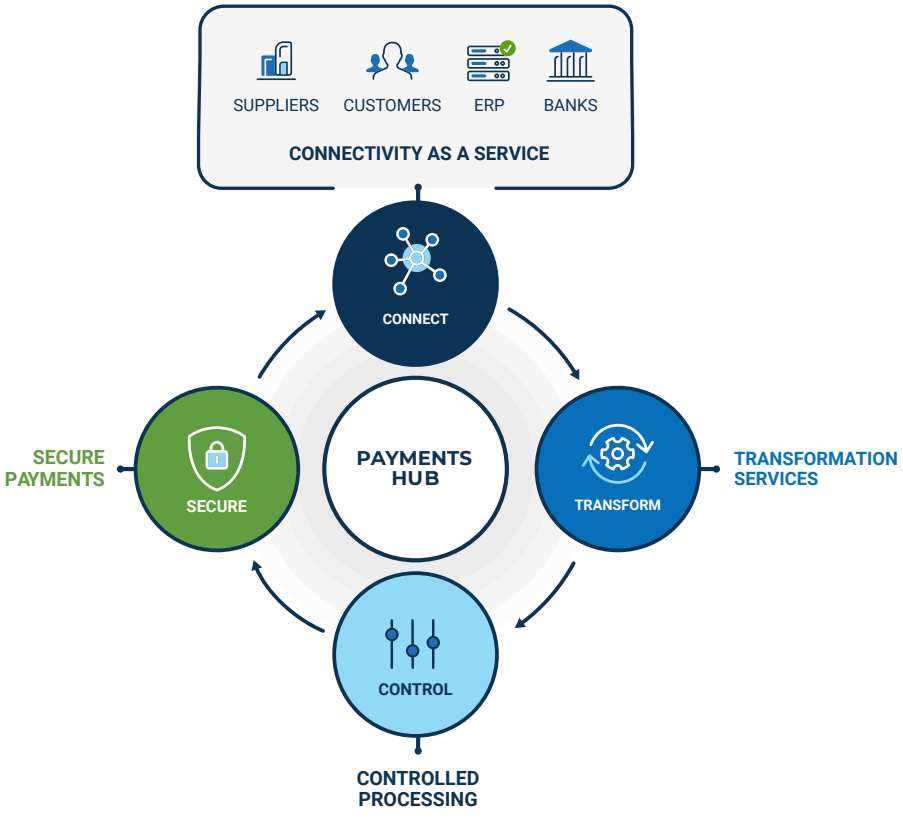
Routing, throttling, retries, cut-off management, and multi-rail decisioning is all managed in one location.

COMPLIANCE:

Rules engines, sanctions screening integration, and audit logging are fully embedded in the payments operation.

DATA & OBSERVABILITY:

End-to-end tracking, dashboards, SLAs, and KPIs help keep treasury teams and CFOs in-the-know about all the payments ins and outs.



4 An Advanced Look: How Payments Hubs Add Strategic Value

For corporate treasury teams, payments are no longer a purely operational function—they are a strategic lever that directly impacts liquidity, risk exposure, vendor relationships, and working capital performance. As payment volumes increase and payment methods diversify, many organizations find themselves constrained by fragmented systems, bank specific integrations, and manual controls. A robust Payments Hub addresses these challenges by providing a centralized, intelligent foundation for managing corporate payments at scale.

At its core, a Payments Hub acts as the single orchestration layer between systems like enterprise resource planning (ERP), procurement platforms, banking partners, and payment networks. By standardizing payment initiation, validation, formatting, routing, and exception handling, a Payments Hub enables treasury teams to execute payments consistently across regions, currencies, and payment types—without duplicating logic or controls for each bank or rail.

Here's a closer look at what businesses can expect with a Payments Hub in place:

Centralized Control and Visibility

A Payments Hub gives treasury a single point of control over all outbound and inbound payments, regardless of source system or bank. This centralization improves real-time visibility into payment status, funding requirements, and exceptions, enabling treasurers to make more informed cash and liquidity decisions. Using a Payments Hub improves cash forecasting accuracy, reduces surprises, and leads to stronger oversight of global payment activity.

Bank and Rail Agnosticism

By separating internal systems from bank-specific formats and connectivity requirements, a Payments Hub eliminates reliance on custom integrations. This allows treasury teams to add new banks, expand into new geographies, or adopt new payment rails with far less complexity. As a result, organizations gain greater flexibility in managing banking relationships, strengthen their negotiating position with banks, and avoid long-term vendor lock-in.

Operational Efficiency and Processing

Standardized validation, enrichment, and repair features improve processing and minimize manual effort. With centralized exception management, treasury and shared services teams can resolve issues more quickly and gain clearer insight into root causes. The result of using a Payments Hub is lower operational costs, fewer payment delays, and stronger internal service levels.

Stronger Risk Management and Governance

A Payments Hub enables consistent enforcement of payment controls—such as approval hierarchies, rules and limits, segregation of duties, sanctions screening hooks, and fraud detection rules—across all payment types and channels. This is especially critical in complex corporate environments with multiple ERPs, business units, and geographies. Using a Payments Hub reduces fraud and error risk, improves auditability, and strengthens internal controls.

Improved Cash and Working Capital Outcomes

With intelligent routing and scheduling capabilities, treasury teams can optimize payments based on value date, cutoff times, urgency, and cost. This allows organizations to hold cash longer when appropriate, avoid late payments, and selectively leverage faster rails when business impact justifies it. A Payments Hub improves working capital optimization and enables more deliberate use of liquidity.

Data Readiness

As banks and payment infrastructures migrate to Nacha 2026 and ISO 20022, richer payment data becomes available — but only if organizations can consume and manage it effectively. A robust Payments Hub normalizes formats and preserves structured data end-to-end. This means businesses improve reconciliation, have fewer investigations, get enhanced reporting, and become better prepared for evolving banking standards.

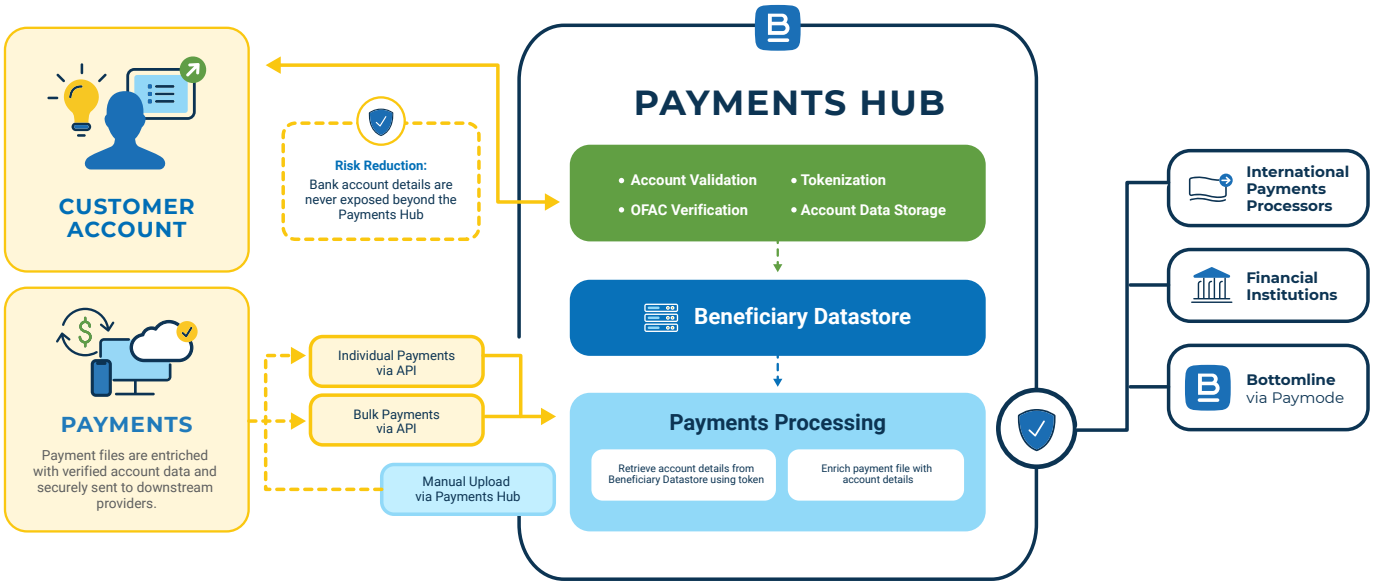
Scalability and Proofing

Whether driven by growth, acquisitions, or geographic expansion, corporate payment complexity tends to increase over time. A Payments Hub provides a scalable architecture that can absorb higher volumes, new entities, and new payment methods without reengineering core processes. Having a robust payments foundation supports long-term growth rather than constraining it.

5 Bottomline's Payments Hub: A Smarter Solution

Bottomline's Payments Hub offers more than basic solutions. With a 35-year background in payments and industry recognition for our **Treasury and Risk Management capabilities,** Bottomline's Payments Hub is built to help businesses reduce compliance risk by centralizing payments, applying automated critical checks, and embedding AI-powered intelligence into day-to-day operations.

The built-in AI agent, Bea, uses a combination of large language models (LLMs) and predictive analytics to surface risks, answer compliance-related questions, and guide decision-making—all within a secure environment where customer data is never passed to public LLMs.



"AI agents like Bea represent the next evolution in enterprise finance, where decisions are data-driven and made in real time. Bottomline's approach to secure, conversational AI is the standard for treasury."

Craig Jeffery, Managing Partner, Strategic Treasurer

Here's a closer look at how Bottomline's Payments Hub helps organizations strengthen their compliance:

1. Automated Sanctions Screening

Bottomline's Payments Hub has built-in sanctions screening, so businesses don't inadvertently pay someone they're not supposed to. This keeps them in line with U.S. and international regulations. The solution imports available data daily, continuously checking beneficiaries/payees and payment instructions against sanctions lists like Office of Foreign Assets Control (OFAC), Specially Designated Nationals (SDN), Blocked Persons List, and others.

Payee beneficiary data can be imported multiple ways, including manually into the solution itself or via application programming interface (API). Once imported, users will be able to easily scan which payees are "Compliant" or "Not Compliant" in the Beneficiary Sanction/Compliance Check column. For unvalidated beneficiaries or Sanction Screening False Positives, users can use their pre-configured workflows to either address, bypass, or override the designated status.

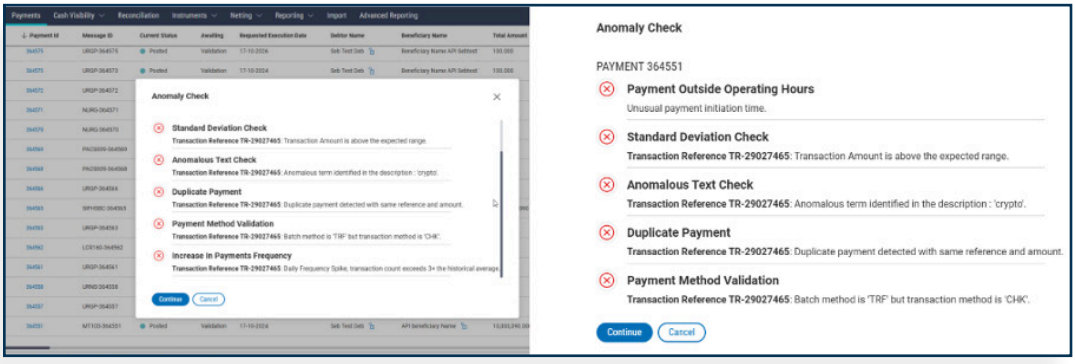
2. AI-Enabled Payments Anomaly Detection

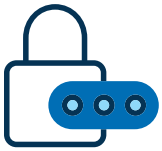
Rules remain the foundation of effective payments anomaly detection, providing the first line of defense against suspicious and abnormal transaction behavior. By codifying known risk patterns, rules enable organizations to detect threats quickly and consistently at scale. When thoughtfully designed and continuously refined, anomaly detection rules help reduce fraud exposure, support regulatory compliance, and create a transparent decision framework that is easy to govern and explain.

Bottomline's Payments Hub automatically detects unusual or suspicious payments behavior which helps flag and stop higher risk transactions before they're initiated.

Here are some of the rules payments teams can build, tune, and optimize in the Bottomline Payments Hub solution:

- **Standard Deviation Threshold Validation –** for each beneficiary, detect transactions that are unusually large compared to historical transaction amounts
- **Suspicious Description Validation –** get alerts about suspicious transaction descriptions or remittance information
- **High-Value Payments to New Beneficiary –** flag high-value payments sent to first-time beneficiaries compared to the global average
- **Duplicate Payments –** detect potential identical payments within or across payment batches
- **Increase in Frequency –** identify unusual spikes in payment frequency (e.g. daily, monthly, yearly) for a beneficiary compared to historical averages
- **Payment Outside Operating Hours –** detect payments initiated at unusual hours or days of the week, based on historical transaction patterns
- **Payment Method Mismatch Validation –** flag discrepancies between the payment method at the batch (or header) level and the payment method at the individual transaction level
- **Real-Time Analysis –** catch suspicious patterns before payments are approved
- **Use Case Scenario Rules –** set up rules for specific industry compliance requirements, such as the Nacha 2026 rules changes
- **Increase in Velocity –** flag if too many transactions occur in a short time
- **Behavioral Analysis –** identify unusual payment amounts or destinations
- **Pattern Recognition –** notice unexpected details, such as repeated failed transactions





3. Account Tokenization

Tokenization replaces sensitive bank account information with a unique code, making it unusable outside the system and reducing fraud risk. Payee and beneficiary bank account data is tokenized, meaning all sensitive data is replaced with a unique, non-sensitive placeholder (or “token”). Outside the system, the token is worthless and unable to be used by bad actors. Tokenization lowers the risk of data breaches, strengthens compliance with data protection regulations and requirements, and allows businesses to process payments without handling actual account numbers.

6

Staying Prepared for Tomorrow: Payments & AI in the Treasury Function

As payment ecosystems modernize and artificial intelligence becomes embedded across financial operations, treasury teams face a dual challenge: keeping pace with regulatory and market change while also positioning the organization for long-term innovation. Preparing for tomorrow's payments environment requires more than incremental upgrades—it demands a deliberate strategy that aligns people, processes, and technology around agility, scalability, and intelligent decision-making.

A future-ready Payments Hub lets organizations absorb change without disruption, leverage data as a strategic asset, and support business growth across regions and models. Three core outcomes define this readiness: regulatory agility, innovation enablement, and scalable global expansion.

Regulatory Agility Across an Expanding Payments Landscape

Regulatory expectations continue to increase in scope and complexity, driven by evolving sanctions, fraud typologies, data and fraud-monitoring standards (such as Nacha and ISO 20022), and regional compliance requirements. For treasury teams, the risk is not simply non-compliance, but operational fragmentation— where controls are implemented differently by channel, bank, or payment type.

A modern treasury payments approach emphasizes centralized policy definition with distributed execution. Rules and controls can be defined once and applied consistently across all payment rails, geographies, and initiation channels. When updates are required—whether due to regulatory change or internal policy shifts—they can be implemented quickly and audited comprehensively.

Key treasury benefits to regulatory agility include:

- Faster response to regulatory change without re-engineering processes
- Consistent enforcement of controls across all payment activity
- Simplified audit preparation and clearer accountability

This level of regulatory agility reduces risk while freeing treasury teams from reactive, manual work.

Enabling Payments Innovation Without Compromising Control

Treasury is increasingly expected to support new business initiatives. At the same time, innovation cannot come at the expense of visibility, governance, or cash control.

A future-ready Payments Hub allows treasury teams to rapidly adopt new payment rails and business models without rebuilding core processes. Whether enabling real-time payments, expanding cross-time payments, or supporting new customer experiences, treasury can act as an enabler rather than a bottleneck.

This is where AI and advanced analytics begin to play a meaningful role. By leveraging richer payments data and intelligent monitoring, treasury teams can:

- Identify anomalies and emerging risks earlier
- Optimize payment routing and timing decisions
- Improve forecasting and liquidity insights

Innovation becomes sustainable when it is supported by standardized processes and intelligent automation.

Scaling for Global Expansion with Consistent Payments Governance

Growth, whether organic or through acquisition, inevitably increases payments complexity. New entities, currencies, banks, and regulatory environments place additional strain on treasury operations, particularly when systems and processes are not updated or designed to scale.

A strong Payments Hub supports multientity, multicurrency, and multijurisdiction operations within a single governance framework. Local flexibility is preserved where required, but global standards remain intact. This balance enables treasury to support expansion without losing control over cash, risk, or compliance.

For treasury teams, this means:

- Faster onboarding of new entities and geographies
- Consistent payment policies and controls worldwide
- Improved visibility into global cash positions and flows

Scalability is not just about handling higher volumes—it is about maintaining discipline and insight as complexity grows.

Looking Ahead

For treasury teams, the convergence of payments modernization and AI represents a pivotal opportunity. By investing in regulatory agility, innovation enablement, and scalable global governance, **treasury can evolve from a transactional function into a strategic driver of resilience and growth.**

7 Payments Hub Glossary

Deepen your understanding of important financial acronyms and phrases relating to **Bottomline's Payments Hub solution.**

= **Benefit of/Supported by Bottomline's Payments Hub**

Account Tokenization

Account tokenization replaces sensitive data like credit card numbers or bank details with a unique, random placeholder (or "token") and is used for data protection and compliance. Tokens have no inherent value, preventing misuse if intercepted, and a secure vault links it back to the real account for authorized transactions.

Account Validation Tools

Account validation tools are used to assess new accounts and changes on existing accounts. These tools can provide much richer data about the account owner, including details such as name, address, balance of the account, and even the IP address associated with the location of the account owner.

ACH

The Automated Clearing House (ACH) Network is a secure electronic network used by U.S. financial institutions to transfer funds between bank accounts. It facilitates both ACH credits (e.g., direct deposit payroll, tax refunds) and ACH debits (e.g., mortgage/utility payments).

AI Agent "Bea"

Bottomline's Artificial Intelligence (AI) agent acts as a digital team member in the office of the CFO, enabling treasurers, cash managers, and compliance professionals to interact with financial data and offer time-saving intelligence.

AML

Anti-Money Laundering (AML) technology uses software, AI, and data analytics to automate and enhance financial crime detection and prevention. May include tasks like transaction monitoring, customer screening, and sanctions checks.

API

An Application Programming Interface (API) is a set of rules and protocols that enables two different software programs to communicate with each other and exchange data. It acts as an intermediary, allowing one application to request services or data from another without needing to understand the internal workings of the other system.

Atypical or Anomalous Activity

Atypical or anomalous activity can come in the form of unusual credit amounts or frequencies, multiple payroll deposits to a single account, sudden changes in payment patterns, and credits inconsistent with historical account behavior.

Controlled Processing

Controlled processing is a function using systems and rules to manage and secure financial transactions. It ensures accuracy, prevents fraud, and optimizes cash flow through real-time monitoring, automated validation, and configurable settlement flows.

Dual Controls

Dual controls require more than one individual to initiate a payment. One individual may authorize the creation of an ACH entry with another confirming the entry and releasing it to the financial institution. Fraudsters may be able to get past one individual, but will have difficulty tricking two.

False Pretenses

"False Pretenses" is a type of financial fraud where a perpetrator misrepresents facts to trick others into authorizing legitimate-looking transactions. This fraud type bypasses traditional authentication checks and relies on social engineering, making risk-based monitoring and anomaly detection critical for prevention.

FBAR

Foreign Bank and Financial Accounts Reporting (FBAR) is a regulatory requirement under the US Bank Secrecy Act that aims to enhance financial transparency, prevent tax evasion, and establish reporting requirements. Any U.S. business that has foreign financial accounts exceeding $10,000 in aggregate at any point during the year must file an FBAR.

ISO 20022

ISO 20022 is an international standard for electronic data exchange between financial institutions. It defines a common language and data format for financial messages so banks, payment systems, and markets can communicate more clearly and consistently. ISO 20022 compliance is mandatory for banks and payment networks.

Machine Learning (ML)

A process that is used to continuously learn from transaction data and adapt to new fraud strategies, rather than relying on static, hard-coded rules.

Micro-Entries

Micro-entries are very small ACH transactions (typically a few cents or less, credit or debit) used to verify that a bank account belongs to the intended recipient and is valid. Micro-entries are not payments and exist solely for account validation, ownership verification, and reducing fraud and errors.

Multi-Factor Authentication

Multi-factor authentication is a security method that requires two or more verification types (or factors) to log into an account, adding layers of defense to block unauthorized access.

Nacha

The National Automated Clearing House Association (Nacha) oversees the ACH Network payment system involving direct deposits and direct payments for all U.S. bank and credit union accounts. Nacha compliance is necessary for all ACH participants in the United States.

OFAC

The Office of Foreign Assets Control (OFAC) is a division of the U.S. Treasury Department that administers and enforces economic and trade sanctions to support national security and foreign policy goals. OFAC compliance is imperative for financial institutions and businesses.

Originator

A Nacha Originator is an entity, company, or person that creates and initiates ACH payment instructions (debits or credits) to a Receiver's account.

Out-of-Band Authentication

Out-of-band authentication validates payment requests or changes to payment instructions by independently verifying the request/change using a method other than the method used by the original request.

Payment Anomaly Tools

Payment anomaly tools are electronic risk management tools that can identify and manage discrepancies in payment transactions. Tools can include anomaly detection, AI-powered solutions, and comprehensive analysis that involve deep learning techniques.

Payment Factory

Payment Factory is a centralized system for managing payment and collection processes, consolidating bank connections, standardizing formats, and automating workflows.

Payment Formats

Payment formats can range from traditional cash and checks to modern digital methods like credit/debit cards, mobile wallets (Apple Pay, Google Pay), bank transfers (ACH), Buy Now Pay Later (BNPL), and cryptocurrency. Each format offers varying convenience, security, and processing speeds.

Positive Pay

Positive Pay is an automated cash management service offered by banks to prevent fraud by matching a company's issued check or ACH payment against actual items presented for clearing. It acts as a security checkpoint, flagging discrepancies like altered amounts or payee names for company review before payment is finalized.

PPD

Prearranged Payment and Deposit (PPD) Entries are an ACH format used specifically for transactions between businesses and consumer accounts. PPD transactions allow businesses to debit (collect) or credit (deposit) funds, such as payroll or monthly bills, based on prior written authorizations.

Risk-Based Audits

Risk-based audits are audits that focus effort where risk is highest, rather than reviewing all processes or transactions equally. The goal is to allocate time, testing, and controls to areas most likely to cause financial loss, compliance failure, fraud, or operational disruption.

Routine and Red Flag Reporting

Red flag and routine reporting is the act of regularly reviewing, reconciling, and reporting on transactions and accounts. Reports can identify new relationships, show transactions of existing customers to new accounts, surface abnormal activity, and verify that transactions are intentional.

Rules-Based Security

Rules-based security is a process set and used by administrators to predefine "if-then" rules to automatically control access, enforce policies, and detect threats.

Sanctions Screening

Sanctions screening is a compliance process where individuals, entities, and transactions are checked against official government and international lists to prevent illicit activities.

Secure Systems and Applications

Systems and applications that ensure maintenance of firewalls and antivirus software is up to date and that all system components and software have the latest vendor-supplied security patches installed.

SFTP

Secure File Transfer Protocol (SFTP) is a network protocol that provides secure file access, transfer, and management over any reliable data stream. SFTP is often seen as a replacement for the traditional File Transfer Protocol (FTP) due to its superior security features.

SOC 2

System and Organization Controls (SOC) 2 is an independent audit of how well a company protects customer data and operates key controls related to security and reliability. It's most required for technology, SaaS, fintech, data, and service companies that handle sensitive client information.

SSO

Integrated Single Sign-On (SSO) is a digital key that grants access to multiple applications with just one set of credentials. Benefits include streamlining access, reducing password fatigue, and simplifying IT management.

SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a global messaging network that banks and financial institutions use to securely exchange payment instructions and other financial information.

Transformation Services

Transformation services is a process that helps organizations shift from slow, manual payments (like checks) to fast, automated payments. This digital technology enables real-time control and security, improved cash flow, and customer demand for instant experiences.

UI

A user interface (UI) is the point of communication between a person and a machine. It's what you see, hear, say, and touch in order to give instructions to a device or receive information back from it. User interfaces dictate how people interact with devices and software.

WEB Debits

WEB debits are internet-initiated ACH debit transactions that are authorized by a consumer and pull money from the consumer's bank account. WEB debit examples include paying a utility, credit card, or subscription bill online via bank account.

Learn more about Bottomline's Payments Hub solution and make your operation more efficient, controlled, and secure.

Contact Us

Bottomline

REV US033026KV

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1 603-436-0700
Toll-free: +1 800-243-2528
info@bottomline.com