Bottomline

A Payments Hub **Fraud & Security Checklist** & Glossary

Payments fraud has become a constant, enterprise-level financial threat, making centralized Payments Hubs with embedded real-time controls essential for reducing risk and standardizing protection across all payment types.

Payments Hub Fraud and Security Checklist

Check all fraud-fighting features that you want in your payments operation

Services & Controls

Validation and Data Integrity

- [ ] ABA Validation
- [ ] IBAN Validation
- [ ] File Encryption
- [ ] Hashed Payment (account information)
- [ ] Hashed Payment File
- [ ] Know Your Customer (KYC)
- [ ] Governmental Checking (e.g. SoS records)
- [ ] Onboarding Process Management

Access Control and Data Protection

- [ ] Tokenization
- [ ] Biometric Authorization
- [ ] Multi-Factor Authentication (MFA)

Verification

- [ ] Direct Verification w / Counterparty
- [ ] Payee Account Ownership (regionally specific)
- [ ] Secure Bank Letters
- [ ] Bank Network Verification (e.g. account owner)

Confirmation and Authentication

- [ ] API Confirmation
- [ ] Open Banking Consent-Based Verification (API)
- [ ] Deposit Validation / Authentication (e.g. microdeposits)
- [ ] Payee Matching, Positive Pay

Rating

- [ ] User Defined Rating Workflow (Risk Scoring)

Monitoring, Interdiction, and Investigation

Screening

- [ ] AML Screening
- [ ] Sanction Checking

Monitoring and Detection

- [ ] Internal Threat Management
- [ ] Anomaly Detection – Data
- [ ] Anomaly Detection – Behavioral Analytics

Interdiction and Investigation

- [ ] Interdiction
- [ ] Audit Trail Management
- [ ] Activity Recording
- [ ] Replay Management

Now what?

If you checked most (or all) of the boxes, you're in good company. Choosing a Payments Hub with the right controls can give your team, organization, and partners greater confidence and peace of mind.

Learn more about Payments Hub via the link below.

Payments Hub

Payments Hub Fraud and Security Glossary

ABA Validation

ABA validation confirms that a U.S. bank routing number is structurally correct and corresponds to a legitimate financial institution.

AML Screening

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

Analytics & Data

Analyzing actions, sequences, frequency, timing, and context of activity to compare current behavior against historical baselines and using analytics and machine learning to surface anomalies or trends rather than relying solely on static rules.

API Confirmation

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.

Audit Trail Management

Audit trail management is the ability to automatically record, store, and manage a complete, time-stamped history of actions, decisions, and system events across financial and operational workflows — ensuring traceability, accountability, and audit readiness.

Bank Network Verification

Bank network verification is a preventive verification control used to confirm that a bank account exists, the account is held at a legitimate financial institution, and the account owner or associated details align with expected records.

Biometric Authorization

Biometric authorization is a method of verifying and approving user access or actions using unique biological characteristics, such as fingerprints, facial features, or other biometric identifiers. It is an access control and authentication measure, grouped alongside multi-factor authentication (MFA) and other verification controls used to strengthen security in sensitive financial workflows.

Deposit Validation / Authentication

Deposit validation / authentication is a method used to confirm that a bank account is active and belongs to the intended owner by validating small test transactions, most commonly through micro-deposits or micro-entries.

Direct Verification w / Counterparty

Direct verification w / counterparty is a control that confirms the authenticity of payment or account information by directly validating it with the counterparty (such as a vendor, supplier, or customer) through an independent, out-of-band communication channel. It is meant to reduce reliance on self-reported or email-based changes and typically strengthens confidence in payment instructions.

File Encryption

Using cryptography, file encryption protects sensitive files by making their content unreadable to unauthorized users.

Governmental Checking

Governmental checking is a verification control that validates entity information by checking official government-maintained records, such as Secretary of State (SoS) business registries, to confirm that an organization is legitimately registered, active, and accurately represented.

Hashed Payment / Hashed Payment File

A hashed payment file is a payment file for which a cryptographic hash value is generated to allow verification that the file has not been altered between creation, approval, transmission, and bank processing.

IBAN Validation

IBAN validation is a data-integrity control that verifies whether an International Bank Account Number (IBAN) is correctly structured and valid according to international standards, helping ensure that international payment instructions reference a properly formatted bank account.

Interdiction

Interdiction is a control that actively delays, blocks, or halts a transaction or action when risk indicators suggest potential fraud, policy violations, or non compliance — before the activity is completed or funds are released.

Internal Threat Management (ITM)

ITM is a security capability used to detect, monitor, and investigate risky or unauthorized activities performed by internal users, such as employees, contractors, or privileged users, that may result in fraud, data misuse, or policy violations.

Know Your Customer (KYC)

KYC is a compliance process used to verify the identity and legitimacy of customers, vendors, or counterparties and assess their associated risk before establishing or continuing a business relationship.

Multi-Factor Authentication (MFA)

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.

Onboarding Process Management

Onboarding process management is the coordinated set of workflows, controls, and validations used to standardize, manage, and govern how customers, payers, vendors, or partners are onboarded into a payments or financial system.

Open Banking Consent-Based Verification (API)

Open banking consent-based verification is a control that confirms bank account or customer information by accessing data directly from a financial institution using secure APIs and only with the explicit consent of the account holder.

Payee Account Ownership

Payee account ownership is a verification that confirms a bank account is owned or controlled by the intended payee or beneficiary, helping ensure that payments are sent to the correct party and not misdirected to fraudulent or unauthorized accounts. In the United Kingdom this is referred to as Confirmation of Payee (CoP).

Payee Matching, 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.

Replay Management

Replay management is the ability to detect and prevent duplicate or replayed payment requests, ensuring that each payment instruction is processed once and only once, even under retries, failures, or malicious replays.

Sanction Checking

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

Secure Bank Letters

Secure bank letters are bank issued documentation, such as Letters of Credit, that provide secure creation, issuance, and management of legally binding bank instruments.

Tokenization

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.

User Defined Rating Workflow

Also known as risk rating, risk scoring, and the evaluation of data reliability, user defined rating workflows are step-by-step processes designed by administrators to evaluate, score, or approve an item so it can transition from a draft state to a final complete state.

Bottomline

About Bottomline

Bottomline helps businesses transform the way they pay and get paid. A global leader in business payments and cash management, Bottomline's secure, comprehensive solutions modernize payments for businesses and financial institutions globally. With over 35 years of experience, moving more than $16 trillion in payments annually, Bottomline is committed to driving impactful results for customers by reimagining business payments and delivering solutions that add to the bottom line. Bottomline is a portfolio company of Thoma Bravo, one of the largest software private equity firms in the world, with more than $184 billion in assets under management.

For more information, visit www.bottomline.com

REV US060426LD

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

Europe, Middle East, Africa Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire RG7 4SA
United Kingdom

Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
emea-info@bottomline.com