FROM TELLER TO MOBILE:
HOW TO STRENGTHEN CHECK FRAUD CONTROLS ACROSS DEPOSIT CHANNELS

As criminals continue to target paper checks to commit deposit fraud, they may exploit vulnerabilities unique to different deposit channels – resulting in gaps in "one-size-fits-all" deposit fraud prevention. Read on for prevention and detection controls specific to each deposit channel that can help you refine your fraud strategy.

RISK VARIES ACROSS DEPOSIT CHANNELS

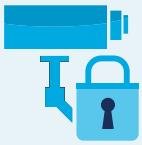
Deposit channels have varying degrees of risk exposure based on processes, technology and other attributes. Criminals are aware of these potential vulnerabilities and may leverage them to commit fraud. For example, identification of an altered check being deposited at a branch relies on teller training and decisioning, while ATMs may have image recognition constraints that limit real-time validation. In addition, multiple deposit channels may be vulnerable to duplicate deposits.

CHANNEL-SPECIFIC CONTROLS CAN HELP REDUCE FRAUD

Customers choose multiple ways to deposit checks with their financial institutions. Deposits typically are made at a branch, ATM, mobile app or occasionally, mailed to the institution. Business customers also may use deposit services provided by their financial institutions, such as remote deposit capture (RDC) or lockbox. A channel-based approach can help manage risk and allow for more targeted controls and resource allocation.

DEPOSIT CHANNEL*	PREVENTION AND DETECTION
 **Branch/Teller**	• Teller training on red flags and deposit fraud trends • Strong ID verification (e.g., an identity can be properly verified, even in a drive-through) • Physical inspection of items (e.g., a UV scanner) • Secondary review for high-value or unusual deposits • Anomaly tracking by teller ID to identify accelerated or inconsistent check acceptance that could be associated with internal fraud
 **ATM**	• Image forgery detection (e.g., pixel analysis, duplicate image detection) • Velocity assessments (e.g., per-item and per-card deposit velocity flags or limits) • Geofencing and device-fingerprinting for mobile apps to flag inconsistencies when comparing to ATM card use location • Risk analysis based on deposit timing, amount and/or ATM location

FROM TELLER TO MOBILE:
HOW TO STRENGTHEN CHECK FRAUD CONTROLS ACROSS DEPOSIT CHANNELS

 **Mobile App** (Smart Phone)	• Device fingerprinting and risk scoring (e.g., operating system, jailbreak, root status, device ID) • Progressive limits (e.g., lower 'new user' limit that increases as trust is established) • Geolocation risk analysis compared to typical use
 **Remote Deposit Capture** (Treasury Management Service)	• Strong customer onboarding, authentication and monitoring (e.g., risk review, multifactor authentication, behavioral analysis) • Image forgery detection (e.g., pixel analysis, duplicate image detection) • Daily, monthly and/or per item limits • Batch anomaly detection (e.g., many checks from new payer) • Periodic customer/user risk assessments and audits
 **Lockbox Service**	• Dual control and security cameras for opening and processing mail/checks • Tamper evident bags and tracking from mail arrival to processing • Limits or threshold alerts for high-risk deposits (e.g., remotely created checks, increased returns and new accounts) • Customer type/baseline comparisons (e.g., irregular pattern compared to peer)
 **Mail/Courier/ 3rd Party**	• Dual control and security cameras for opening and processing checks • Payee verification (e.g., verify abnormal/first time deposits with customer) • Physical inspection of items (e.g., UV scanner) • Increased review for high value, frequent returns or unusual deposits

FROM TELLER TO MOBILE:
HOW TO STRENGTHEN CHECK FRAUD CONTROLS ACROSS DEPOSIT CHANNELS

All Deposit Channels	• Image quality standards for the front and back of the check (e.g., MICR legibility and endorsement verification) • Automated duplicate and high rate of return detection against previously processed images across the institution and available consortium data • Positive pay/reverse positive pay and payee name matching • Real time scoring engine that ingests channels signals (device, location, teller notes, MICR) and triggers holds or manual review • Customer education: clear messaging about safe check usage, mobile deposit best practices and how to report suspicious checks

**Note: The items listed above are examples for consideration. This table is not intended to provide an inclusive list of all practices to prevent deposit fraud.*

CONCLUSION

Assessing deposit trends and fraud controls based on deposit channel – as well as regularly reviewing fraud trends – can help identify potential vulnerabilities and lead to more precise and proactive check fraud prevention and detection.

The check fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about check fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.