White Paper

It's Time for a More Holistic Approach to Fraud & Compliance Risk Management

effectiv

November 2022

effectiv

It's Time for a More Holistic Approach to Fraud and Compliance Risk Management

A guide for community banks and credit unions

Fraud risk and compliance risk: different sides of the same coin or merely two points on the broader risk spectrum? Increasingly, it is becoming harder to delineate between fraud risk and compliance risk—and the resulting threats to financial institutions' reputation, customer experience and bottom line.

Increasing consumer expectations for speed, accuracy and convenience and the resulting race toward digitalization have also expanded the speed with which bad actors such as identity fraudsters and money launderers move to exploit gaps within financial crime risk management systems. And community banks and credit unions are at even greater risk as fraudsters increasingly target them due to big bank competitors' continued investments in enterprise risk management tools and strategies.

This protection gap has been compounded by ever-increasing compliance regulations and the race to head off new threats. As a result, many community-based financial institutions' risk management tools now consist of a disjointed collection of point solutions and siloed risk management functions. But, as the lines begin to blur between different types of risk, continuing a disjointed approach to fraud and compliance risk management will inevitably result in missed vulnerabilities to be exploited by malicious actors ready to pounce.

It's time for a fresh approach to risk mitigation—one that's seamless, integrated and cost-effective.

Types of Risk

At a high level, the primary types of risk affecting financial institutions include cyber risk, compliance risk and fraud. We'll break each type of risk down into more detail and then explain why a more holistic approach to managing all of them is necessary and beneficial.

Cyber Risk

Cyber attacks against financial institutions (FIs) jumped 238 percent in 2020[1] costing the financial sector $5.72 million on average per data breach.[2]

According to cybersecurity firm UpGuard, the top six current threats to financial institutions[3] come from:

1. **Phishing** – tricking end-users into divulging login credentials including usernames and passwords.

2. **Ransomware** – cybercriminals infect a user's or organization's computer systems with malicious code, locking the user or organization out of the system and demanding a ransom be paid to restore access.

3. **Vulnerability** exploits – malicious actors exploit known or undiscovered vulnerabilities in developer tools or other software that provide them access to a user's or organization's systems.

4. **Distributed Denial-of-Service** attacks (DDoS) – cyber criminals hijack an organization's servers by flooding them with fake connection requests, and taking them offline. Criminals can either exploit the opportunity to launch other attacks while IT departments scramble to get systems back online or request a ransom to restore systems.

5. **Supply Chain** attacks – Malicious actors attack third-party vendors servicing financial institutions that may have fewer cyber risk protections place, creating possible inroads into financial institutions' more sensitive resources.

6. **Bank Drops** – fake bank accounts used by cyber criminals opened using stolen customer credentials to store stolen funds.

Regulatory/Compliance Risk

Every financial institution is painfully aware of the staff, time and money resources needed to maintain regulatory compliance. One estimate shows an average increase in U.S. banks' non-interest expenses of $50 billion dollars per year since the passage of Dodd-Frank[4] and another shows compliance costs can mount to $10,000 per employee[5]. These increases can be directly attributed to increased fraud related to greater digital demand[6].

---

1 VMWare, "Modern Bank Heists 3.0," May 2020.

2 UpGuard, "10 Biggest Data Breaches in Finance," Aug. 22, 2022.

3 UpGuard, "The 6 Biggest Cyber Threats for Financial Services in 2022," Aug. 29, 2022.

4 Forbes.com, "The Creeping Cost of Compliance," Oct. 21, 2021.

5 Ibid.

6 Ibid.

Examples of the types of regulatory compliance financial institutions must manage include:

- **KYC/CDD** – Part of the onboarding process involves managing Know Your Customer (KYC) guidelines which are designed to protect financial institutions against fraud, corruption, money laundering and terrorist financing by setting acceptable standards for verifying customer identities and fund sourcing. Customer Due Diligence (CDD), a subset of KYC, is used by financial institutions to collect and evaluate relevant information about a customer or potential customer to establish identity and perform checks against sanction lists and other public and private third-party data.
- **AML –** Part of the Bank Secrecy Act (BSA), anti-money laundering (AML) compliance helps financial institutions uncover suspicious activity associated with criminal financial acts, including money laundering and terrorist financing. AML compliance requires financial institutions to submit Suspicious Activity Reports (SARs) to notify the government when suspicious activity is detected.
- **Privacy** – Financial institutions are required to protect the privacy of financial information under Gramm-Leach-Bliley which governs how personal financial information can be collected and disclosed; the Safeguards Rule, which requires FIs to maintain safeguards to protect customer information; and another provision to prevent entities from gaining access to consumers' personal financial information under false pretenses.

- **Credit/Lending** – Financial institutions are required to perform lending activities according to a plethora of compliant procedures related to the issuance and maintenance of loans and credit covering everything from how they may target consumers to how they make approval and denial decisions to how much credit to extend and what fees can be collected to repayment terms, collection activities and much more.

Fraud Risk

Fraudsters are continually finding new and creative ways to stay one step ahead of FI fraud controls—and the proliferation of digital activity has brought an explosion of increased attacks.

Financial institution fraud is at an all-time high and it's only expected to increase:

- Identity fraud losses reached $24 billion in 2021 — a 79% increase over 2020[7]
- New account fraud increased 109%[8]
- Traditional identity fraud cost individual victims $1,551 in 2021[9]

Types of fraud incurred by FIs include:

- **New account fraud** – New account fraud occurs once a malicious actor has successfully surpassed a financial institution's KYC/CDD and/or BSA/AML regulatory controls at onboarding. It can occur as a result of first-person identity fraud, third-person identity fraud (using stolen identification credentials) or synthetic ID fraud (a unique identity built from disparate parts of real and stolen identities as well as some fake information).
- **Application fraud** – Application fraud occurs when an existing customer opens a new account or obtains a loan using fraudulent information.
- **Transaction fraud** – Transaction fraud occurs when a criminal attempts to defraud a financial institution or customer using a transaction such as person-to-person (P2P) payments, ATM transactions, wire transfer, ACH, check fraud or remote deposit capture (RDC) fraud.
- **Account takeover** – Account takeover schemes are largely the result of phishing scams designed to trick consumers into divulging banking credentials which give cybercriminals access to online account usernames and passwords.

The Problem with a Siloed Approach to Different Types of Risk

There's no question that different types of risk call for different approaches, but how different? Instead of thinking about these various types of risk as standalone (and taking a siloed approach to detection and prevention), what if we considered each type of risk as merely a point on a larger risk continuum and thought about ways to more efficiently—and effectively—create strategies, build our risk organizations and detect/prevent against threats from all risks?

As threats continue to escalate from all points (cyber, compliance, fraud), the distinction between the different types of risk becomes increasingly blurry. A loss that starts as a compliance threat can eventually end up as a fraud threat—threatening losses on two fronts: regulatory fines and hard-dollar losses from fraud.

7 Help Net Security, "Traditional identity fraud losses soar, totalling $52 billion in 2021," April 5, 2022.

8 Ibid.

9 Ibid.

For example, someone using a synthetic ID to open a new account has bypassed KYC/CDD controls (a compliance threat). Later, after nurturing the banking relationship and opening and maxing out a line of credit, they fall off the radar without paying, leaving the FI with a write-off (a fraud loss). The financial institution faces a two-pronged threat from a single incident.

In another example, cybercriminals may target an FI's customer base from a hacked email list (a cybersecurity threat) and send out phishing emails in an attempt to acquire as many online banking user credentials as possible to gain access to accounts and funds (fraud risk), as well as build an arsenal of identifying information that can be sold on the dark web and/or used to build synthetic identities for use in future fraudulent activities (future compliance, fraud and cyber risk).

It's becoming clear that FIs must reengineer risk management strategies and systems to gain full visibility into operations—detection and prevention systems must be leveraged to full efficiency and risk management teams must be reading off the same page. At the same time, systems and strategies must be nimble enough to meet continually evolving compliance standards as well as the rapidly changing and expanding threat landscape. Finally, FIs must be continually aware of risks to accountholders and employee experiences. None of these goals can be achieved using siloed point solutions that must be managed and maintained separately, despite using many, if not all, of the same inputs.

Holistic Risk Management Using a Single Platform

Industry analysts agree that an integrated approach to managing all types of risk (or as many types as possible) in an integrated fashion is the direction financial institutions should be heading.

In a regulatory advisory, KPMG recommends strengthening "integration of compliance within the business, taking advantage of opportunities to embed compliance resources and new functionalities alongside large operational shift[10]," as a key tactic to overcome compliance risk challenges.

The good news is that expensive investments in enterprise fraud and compliance solutions aren't necessary. While the largest financial institutions may require more sophisticated enterprise systems or a suite of best-in-class point solutions with expensive custom

10 KPMG, "Compliance risk challenges in financial services," 2020

integrations, most community banks and small to mid-sized credit unions can leverage a single platform to perform both fraud detection and prevention and compliance checks at the same time.

Here is the minimum functionality required of a financial crime solution to leverage fraud and compliance risk mitigation from a single solution:

- Integration with trusted third-party data intelligence providers so the system works in the background to confirm that all the data input by applicants checks out when compared against publicly available information sourced from a wide range of records and digital resources before a consumer is onboarded.
- The ability to leverage integration with third parties that perform checks against government watch lists and sanction lists for AML compliance.
- Automated ongoing transaction monitoring to flag high-risk actions or high-value transactions that may signal money laundering, terrorist or other criminal activity.
- Integrated machine learning (ML) to perform large volumes of account opening, application, transaction and payment transaction monitoring in near real-time with the highest degree of accuracy.
- A proven track record of delivering highly accurate results to zero-in on suspicious activity while eliminating friction and lost business due to false positives, thereby ensuring a top-notch consumer and employee experience.

- The ability to customize and refine risk profiles based on a financial institution's unique risk tolerance level and operating environment.

The Effectiv Platform – A Single Solution for Fraud and Compliance Risk Management

Effectiv is one of the only platforms that community-based banks and credit unions can use for both fraud detection and prevention, and compliance–all in a unified solution.

Effectiv's turnkey, customizable application and onboarding fraud detection and compliance automation platform checks all the above criteria and more to stop fraud at the source while minimizing friction for legitimate applicants because its ML capabilities help eliminate false-positives—at a fraction of the cost and time to implement as expensive enterprise solutions.

Where enterprise solutions can take 6 to 12 months to implement and fine-tune, Effectiv's platform comes already integrated with trusted third-party data intelligence providers. It can be deployed out of the box with built-in rules or customized so rules can be added, deleted or adjusted based on your FI's unique risk profile and tolerances. Better still, customizations are as easy as drag and drop and don't require any intervention from IT, engineering staff or programmers, further lowering the total cost to own and maintain the solution.

And the financial benefits extend beyond bottom-line efficiencies, mitigated fraud losses and compliance. Financial institutions can heavily impact top-line revenues by eliminating false positives that risk abandonment from legitimate account holders. On the other hand, failing to identify potential fraud or compliance threats can have catastrophic consequences. The Effectiv platform is an elegant solution that gives community banks and credit unions the best of both worlds—stop fraud in its tracks and remain compliant while enabling business continuity, all while reducing costs and increasing revenues at an affordable price point.

The Effectiv platform protects in real-time across all channels wherever fraudsters attempt to strike: new account applications, loan applications, suspicious activity, credit card transactions and P2P payments. A single, unified solution provides full coverage and protection.

Effectiv makes it easy to stop financial crime effectively, offer a better account holder and employee experience, protect revenue and achieve market differentiation.