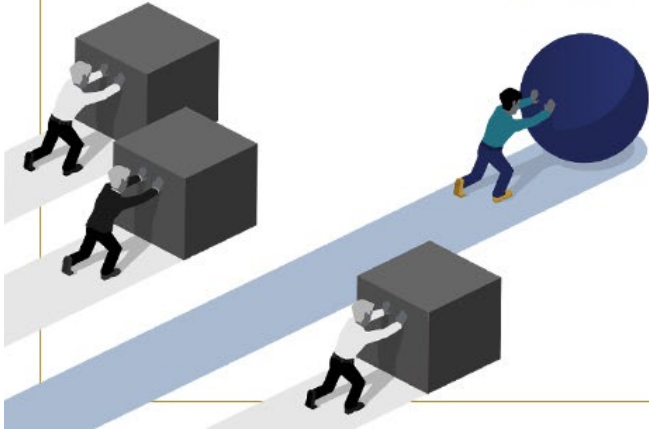


FRAUD MANAGEMENT COMPLIANCE & THE RISKS ISSUERS FACE BY "DOING IT YOURSELF"



By Jennifer Marshall & Julia Lum

One of the most overlooked and misunderstood areas in banking is how internal operations place issuers at risk for noncompliance when investigating and resolving fraud claims.

Adding more resources toward fraud management is a tough sell internally since it's typically viewed as a non-revenue generating, unavoidable loss line. Unfortunately, what little investment FIs do make in improving their fraud investigation and decisioning processes tends to only exacerbate the organization's financial losses.

Investing in "DIY" solutions results in lengthy operational disruption and non-scalable improvements that only put issuers at more risk of falling out of compliance. Additionally, existing fraud management processes are largely shaped on outdated practices inherited from legacy employees (the unnecessary practice of requiring accountholder signatures at intake comes to mind).

Recognizing the compliance risks of trying to solve fraud management inefficiencies internally will help team leaders make the business case for implementing third-party fraud management SaaS solutions.

The Regulations Governing Fraud Claims

The two primary banking regulations that come into play during a fraud and dispute investigation are Regulation or "Reg" E (Electronic Fund Transfer Act) and Regulation or "Reg" Z (Truth in Lending Act). Debit transactions fall under Reg E, which mandates that financial institutions have ten days to either make a final case decision or provide provisional credit; if issuers take the latter action, they have 90 days to resolve the dispute. Credit transactions are governed under Reg Z. These dispute deadlines depend on the last statement date, as well as when the claim was submitted to the customer's issuing bank. These dates result in highly incongruous timeframes in which a Reg Z dispute must be resolved. Nevertheless, Reg E disputes tend to be more challenging to resolve than Reg Z disputes due to the simple fact that money involved in Reg E disputes is real.

Is upholding this compliance *really* so important?

Yes. It only takes one fraud ring or a series of attacks to overwhelm a back-office team of investigators and prevent them from upholding regulatory time frames. If auditors determine that an issuer is unable or unwilling to follow government regulations, the government issues fines and penalties. Reg E and Reg Z fines

are typically \$1000 per violation, not to exceed 1% of a financial institution's total assets. In more extreme cases, when a financial institution fails to comply, it can also be issued a Consent Order. A Consent Order is the OCC's last effort to force a financial institution to comply with regulations. If the Consent Order is not followed, the FDIC has the authority to shut down the financial institution in question.

To underscore just how much of a problem compliance is in the banking world, just look how many institutions are currently under consent order by the OCC.

Why is upholding chargeback compliance so hard?

Financial institutions face a considerable challenge in upholding compliance with government regulations and network mandates when carrying out the fraud and dispute management process. While evolving digital platforms diverge from conventional banking, it is essential to note that traditional banks' federal regulatory guidelines still apply to modern card issuance companies. Not to mention the significant strain on financial and human resources required to understand, apply, and continuously update processes that meet regulatory requirements.

Reg E, Reg Z, Nacha, and card network mandates use many reason codes and rules stipulating everything from debit card issuance, provisional credit, online merchandise, and unauthorized transfers. However, the solutions that issuers employ for managing fraud claims remains largely undefined, leaving FIs with the sole responsibility (and risk) of managing fraud while facing the following challenges:

1. Manual Workflows

Many financial institutions manage disputed transactions with a combination of spreadsheets, emails, forms, and paper trails of decision trees. Issuers with manual processes rely heavily on their employees to define, uphold, and update complex workflows – all within mandated deadlines. Considering the ongoing regulatory and network-mandated updates, along with the plethora of sources from which to gather case information (e.g., account holders, networks, merchants, and core banking platforms), manual workflows are guaranteed to impact your organization negatively.

2. Human Error

Manually prioritizing and working disputes can be a daunting prospect if employees lack a thorough understanding of the industry's complexities or intuitive software with which to store information. Without seasoned fraud and dispute experts and/or automated workflows, information gathering, issuing provisional credit, and adhering to regulatory deadlines are often disorganized and prone to human error. Financial institutions mistakenly believe their dispute resolution processes are compliant until an audit determines otherwise.

3. Limited Scalability

Manual, complex internal fraud management solutions simply cannot scale to support the economic reality we face today. Internal solutions are overly dependent on people to scale and meet growing business needs. Biannual mandates rely on internal IT resources and influxes in claim volumes rely on additional back-office staff. All of which requires budget approval for increasing the resources allocated on a non-revenue generating program. Lack of funding and staff cuts puts financial institutions at risk for noncompliance.

How Strategic Partnerships Eliviate the Burden of Compliance

Investing in fraud alerts and detection does not solve compliance issues. There will always be fraud and there will always be actions federally required to solve for fraud post-authorization. Strategic partnerships can help. Implementing cloud-based, scalable technology like [ARIA®](#), [Quavo's automated fraud management investigation and decisioning tool](#), eliviates the burden of upholding compliance with limited resources. [Banks](#)

are increasingly streamlining their fraud and dispute management processes with fintech solutions, proving that mitigating risk isn't something issuers must face alone.