

The Credit and Financial Management Review

The Journal for Credit and Financial Executives

Volume 30, Number 2

Second Quarter 2024

- The Dynamic Fort Knox Concept
- The Propriety of Monetizing Preference Claims:
Another Circuit Court Weighs In
- Name That Economy



**Credit Research
Foundation**

The Credit and Financial Management Review

A
Journal
for
Credit
and
Financial
Executives

Copyright© 2024 by Credit Research Foundation Inc. Westminster, MD

All rights to this material are reserved.

No part of the material may be reproduced in any manner whatsoever
without written permission from the Credit Research Foundation.

Contents

- 5 *The Dynamic Fort Knox Concept*
By: Ali Kidwai, Lilly Filippov, and Nathaniel Stickman, Bectran
- 22 *The Propriety of Monetizing Preference Claims:
Another Circuit Court Weighs In*
By: Eric S. Chafetz & Brittany M. Clark, Lowenstein Sandler LLP
- 36 *Name That Economy*
By: Steven C. Isberg, PhD, Senior Fellow, Credit Research
Foundation and Chair, Dept of Accounting, Towson University

Editorial Staff		
Mike Bevilacqua Executive Editor	Matthew W Skudera CRF President	Cheryl L Weaverling Associate Editor

The Credit and Financial Management Review is published quarterly by the Credit Research Foundation
Submissions of articles or advertising opportunities should be directed to:

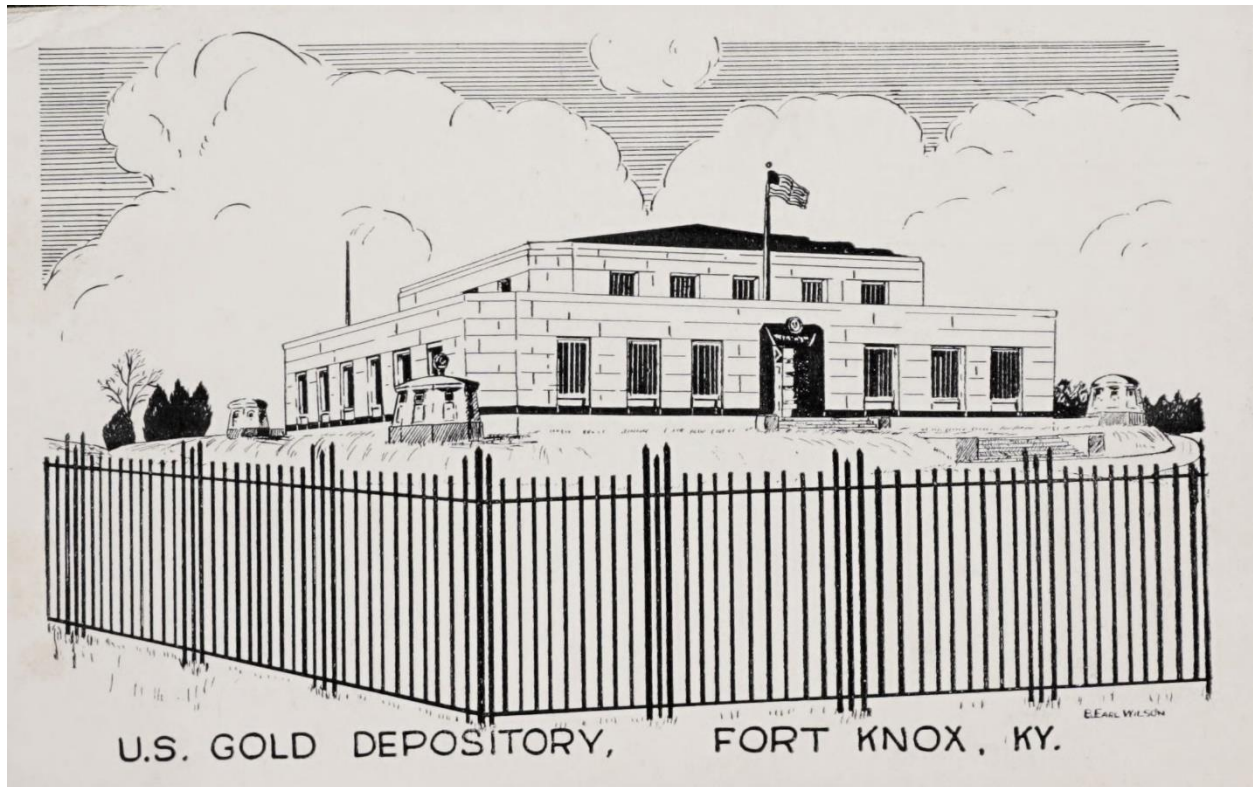
Mike Bevilacqua, Executive Editor
Credit Research Foundation
1812 Baltimore Blvd., Suite H
Westminster, MD 21157-7146
Mikeb@crfonline.org

The Dynamic Fort Knox Concept

*By: Ali Kidwai, Lilly Filippov, and
Nathaniel Stickman, Bectran*

Abstract

It is important for credit managers to focus on the credit risk of a potential customer, but it is equally important to guard against fraud risk and identifying creative scammers. This article will help you stay ahead of financial risks and build your own “fortress” against scammers who are siphoning revenue from your bottom line.



Imagine your credit department running like a well-oiled machine. Sales are up, approvals are quick, and everything seems perfect. Then, out of nowhere, a fraud attack hits. When you try to trace it, you find a trail of lost efficiency and seeping revenue.¹ You're left wondering, "How did this happen?"

Credit and payment fraud are pervasive issues within every industry, capable of severely impacting an organization's operations and cutting into its income.² Fraudsters leech away at your business in small sums here and there, making their schemes hard to detect and prevent. Despite that, an organization can set up strategies to effectively mitigate fraud.

Enter the Dynamic Fort Knox concept. Think of it like building your own fortress— not just a set of walls, but a defense system that's smart, adaptable, and ready for anything. Your Dynamic

¹ A 2024 report by the Association of Certified Fraud Examiners (ACFE) estimates that organizations lose on average five percent of their revenue to fraud and that each fraud case lasts a year without detection. <https://www.acfe.com/-/media/files/acfe/pdfs/rtn/2024/2024-report-to-the-nations.pdf>

² In a survey by the Association for Financial Professionals (AFP), 80% of organizations reported being targets of payment fraud in 2023. <https://www.afponline.org/docs/default-source/registered/2024-afp-payments-fraud-survey-key-highlights.pdf>

Fort Knox can be whatever you need it to be—whether a massive, impenetrable fortress or a quick, agile outpost.

In this article, you’re going to see the importance of having an effective credit fortress—and steps for building your own. We’ll dive into real-world examples and practical tips to help you stay ahead of financial risks and revenue siphons. By the end, you’ll know exactly how to turn your credit department into an unbreakable, yet flexible, stronghold.

Nature of Fraud Risk

Differences in Evaluating Fraud Risk and Credit Risk

A credit manager’s default inclination is to always focus on assessing the credit risk of a potential customer. This includes:

- Trade/bank references
- Bureau reports such as Experian, Equifax, Dun & Bradstreet, etc.
- Personal credit scores from TransUnion, Experian, etc.
- Purchase history and payment behavior

While these assessments are key to targeting credit risk, they fail at identifying creative scammers. Those scammers make it a point to prey on any credit departments inadequately equipped with the kinds of tools and policies necessary for effective fraud checking.

Two additional factors keep credit departments from effectively responding to fraud. First, fraud risk is significantly less frequent than credit risk, and cannot be boiled down to a set of predefined checks, which is what these bad actors take advantage of. Credit managers fail to put emphasis on the impact of fraud risk due to its low occurrence relative to credit risk. That causes organizations to suffer when fraud does occur.

Second, fraud picks at an organization with a few dollars here, a few dollars there. Organizations take this to mean that fraud isn’t costly, but that’s part of the fraudster’s strategy. Credit managers again fail to give fraud risk adequate concern, and bad actors use that fact to allow them to keep coming back.

That’s “just the tip of the iceberg,” however. Once a scammer finds an avenue to steal funds, you can be sure they’re also stealing company and customer information—which they may subsequently trade on the black market. Fraud quickly becomes less about the currency and more

about making sure you protect your information and the information of the customers who trust you.

Given these facts, it is imperative that organizations develop a dynamic mentality to build themselves a fortress to tackle these issues.

How Fraudsters Target Weak Credit Departments

Fraud has numerous ways that it can attack. Scammers look for credit departments whose defenses allow even one of their tactics to get through. Once they find a way in, these tactics all allow fraud to sap your cash flow, operations, and guarded information.

Common Tactics

The age-old fraud tactics are still in play. They can be easily identified with simple checks, but credit departments still need to be watching for them.³ A few examples include:

- Identity theft
 - o Impersonating legitimate person(s) and businesses using stolen drivers licenses, social security numbers, company documents, etc.
- Forging documents
 - o Carefully creating dubious documents such as W-9s, purchase orders, and shipping verification documents
- Email domain impersonation
 - o Masquerading as a legitimate business by changing a few letters in the domain, such as “xyzdistribution.com” when the legitimate domain is “xyzdistributions.com”

Novel Tactics

However, today scammers additionally employ extremely creative tactics to trap credit departments. These are, in contrast to the age-old tactics, extraordinarily difficult to catch, and only the most well-prepared credit departments will see them coming. These include:

³ The AFP’s 2024 survey, for instance, finds that 40% of organizations were underprepared for compromised business email addresses, a common fraud tactic.

- Bust-out scheme
 - A fraudster may begin by making a series of small, legitimate purchases, typically in quick succession and paid for with cash. Once a good reputation is established, the con artist makes a set of legitimate seeming larger purchases, which will not be paid.
- ACH ghost funding
 - A scammer funds an account using an ACH transfer. The individual does not have sufficient funds, but they have chosen an account provider that does not prevent actions being taken on funds before ACH transfers “settle” and the inaccuracy is detected. The fraudster can thus promptly make a purchase using the “ghost funded” account.
- Refunds and chargebacks
 - A bad actor fabricates a charge or charges (often small) on their account by photoshopping receipts and bank statements. The individual then submits the manipulated documents as proof to a credit department. In an effort to provide good customer service, credit departments may proceed to issue refunds for the nonexistent charges.

Use Case — Double Trap⁴

Fantastic Flooring was hit with fraud. The scammer used an email domain impersonation to trick an employee into thinking the scammer was a trusted customer. The customer, Impressive Inns, used the domain name “impressiveinns.com”; the faked domain was just one letter different: “impressiveinn.com.”

When Fantastic Flooring assessed the damage, the company was surprised to find how much chaos the fraud had left. The scammer had been working them for over a year, taking small amounts here and there, but they added up.

More painfully, the scammer had access to valuable customer information. The worst was how much they learned about Impressive Inns, but Fantastic Flooring couldn’t be sure what other customers’ information the fraudster had stolen. The company would have to alert several customers about the breach.

Fantastic Flooring responded with a rigid fortification. They adopted a series of predefined checks to prevent common fraud tactics. The company didn’t grasp the need for dynamic defenses, however. Because of that, it was unprepared for more novel fraud tactics.

⁴ While this situation is based on observed real-world fraud cases, names and other details have been changed.

A second scammer saw the opportunity. With a set of photoshopped receipts, the fraudster showed up requesting a refund. Everything else seemed valid. The fraudster hadn't faked a domain name or used any of the other common tactics that Fantastic Flooring had prepared for.

Fantastic Flooring wanted to provide good customer service, especially since their rigid fortifications had made transactions more of a headache for their customers. So, the credit manager approved the refund—and the scammer had found a way in.

How to Build Your Fort Knox — Components of a Good Fraud Prevention Strategy

A solid fortress is secure on all fronts and has defined exit and entry points that exist to validate and neutralize (if needed) all incoming parties. Similarly, a strong credit department must implement policies that dynamically prevent fraud, like the policies detailed below.

A fortress is only as effective as the army inside it, however. In terms of culture, it is imperative to train your credit team to always be on the lookout for fraud. The most effective teams are equipped with a set of tools for validating business information.

A truly dynamic fortress needs effortless defenses. Automatic security measures and validations keep your organization nimble. Advanced alerts make a team more capable of seeing and catching fraud, and also adaptable enough to provide a good, seamless customer experience.

Strategies & Policies

Implementing effective strategies and policies is essential for creating a fraud prevention framework that aligns with the Dynamic Fort Knox concept. This approach ensures a fortified, adaptable defense against evolving fraud threats.

- Clear anti-fraud policies
 - o Defined procedures: Establish clear procedures for handling suspected fraud cases, including reporting and escalation processes.
 - o Regular updates: Keep policies up-to-date with the latest regulatory requirements and industry standards.
- Employee accountability
 - o Roles and responsibilities: Clearly define roles and responsibilities related to fraud prevention to ensure accountability.
 - o Incentives for compliance: Offer incentives to employees who consistently follow fraud prevention protocols and identify potential fraud.

- Customer verification
 - Enhanced due diligence: Implement enhanced due diligence for high-risk customers, including additional verification steps and closer monitoring.
 - Regular customer reviews: Conduct periodic reviews of customer information to ensure it remains accurate and up-to-date.
- Incident response plan
 - Crisis management team: Establish a crisis management team dedicated to responding swiftly to fraud incidents.
 - Communication protocols: Develop communication protocols for informing stakeholders and customers in the event of a fraud incident.
- Data analytics
 - Behavioral analysis: Use behavioral analysis to identify unusual patterns that could indicate fraud.
 - Predictive modeling: Implement predictive modeling to forecast potential fraud risks and proactively address them.

Tools & Data


The right strategies and policies don't effectively prevent fraud on their own. To implement the Dynamic Fort Knox concept, using the right tools is vital. These make credit teams more adaptable and quicker to catch fraud before it's intruded on your organization. The following tools can be deployed at all stages of the order-to-cash process to alert users to the possibility of fraud.


- Credit onboarding
 - SOS/OFAC/TIN checks
 - Bank account funding verification
 - Identity checks (driver's license, SSN, etc.)
 - IP address and geo-lookup
 - Email verification (e.g., verifying domain authenticity)
 - Biometric verification (e.g., facial recognition, fingerprint scanning)
- Payments
 - Blacklisted IP database
 - Stolen credit card and ACH database
 - Bot/spam executions checks
 - Transaction velocity monitoring (detecting rapid transactions in a short period)
 - Two-factor authentication (2FA) for payment approvals
- Purchasing
 - Shipping address verification (USPS, FedEx, etc.)
 - PO number verification



O2C Fraud Alerts

Tools for safeguarding your customers from fraud



 Credit Onboarding	 Payments	 Purchasing
<ul style="list-style-type: none"> ✓ SOS/OFAC/TIN checks ✓ Bank account funding verification ✓ Identity checks (driver's license, SSN, etc.) ✓ IP & address and geo-lookup ✓ Email verification/ domain authenticity ✓ Biometric verification (e.g., facial recognition) 	<ul style="list-style-type: none"> ✓ Blacklisted IP database ✓ Stolen credit card and ACH database ✓ Bot/spam executions checks ✓ Two-factor authentication (2FA) for payment approvals ✓ Transaction velocity monitoring (detecting rapid transactions in a short period) 	<ul style="list-style-type: none"> ✓ Shipping address verification (USPS, FedEx, etc.) ✓ PO number verification

For more information: www.bectran.com


Automation

Automation is a cornerstone of the Dynamic Fort Knox concept, playing a crucial role in enhancing the efficiency and effectiveness of fraud prevention across all stages of the order-to-cash process. By leveraging advanced technologies and automated systems, businesses can proactively identify and mitigate fraud risks, ensuring a secure and seamless experience for both the company and its customers.

Automated risk management needs to operate as your credit team's best friend. Automated systems rely on checks and tuning from credit managers who know the customer base, and who are often the first to see new threats emerging.


Below are examples of how automation can be integrated into various stages of the order-to-cash process:




- Credit onboarding
 - Automated document verification: Use OCR (Optical Character Recognition) and AI to automatically verify identifying documents such as driver's licenses and passports.
 - Real-time data validation: Integrate with external databases (e.g., government databases, credit bureaus) to instantly validate customer information and reduce manual checks.
 - Risk scoring models: Deploy AI-driven risk scoring models that analyze multiple data points to assess the fraud risk associated with new applicants.
- Payments
 - Transaction monitoring: Implement automated systems that monitor transactions in real-time, flagging suspicious activities based on predefined rules and machine learning algorithms.
 - Fraud detection algorithms: Utilize advanced algorithms to detect patterns indicative of fraudulent behavior, such as unusual spending patterns or multiple failed login attempts.
 - Automated chargeback management: Streamline the chargeback process by automating the collection and submission of evidence to dispute fraudulent claims efficiently.
- Purchasing
 - Supplier verification: Automate the verification of suppliers by cross-referencing with trusted databases, ensuring the legitimacy of business partners.
 - Purchase order matching: Use automated systems to match purchase orders with invoices and delivery receipts, identifying discrepancies that may indicate fraud.
 - Inventory management: Implement automated inventory tracking to detect unusual patterns that could suggest theft or fraud.



O2C Fraud Automation

How to leverage automation to proactively identify and mitigate fraud risks



 Credit Onboarding	 Payments	 Purchasing
<ul style="list-style-type: none"> ✓ Use OCR to automatically verify documents like DL and passports ✓ Integrate with external databases to instantly validate and reduce manual checks ✓ Deploy AI-driven risk-scoring models for multiple data point analysis 	<ul style="list-style-type: none"> ✓ Implement transaction AI monitoring to flag suspicious activities ✓ Use AI algorithms to detect patterns indicative of fraudulent behavior ✓ Automate chargeback processes to dispute fraudulent claims efficiently 	<ul style="list-style-type: none"> ✓ Automate cross-referencing for business verification ✓ Automate purchase order to invoice matching ✓ Automate inventory management

For more information: www.bectran.com

Balancing Customer Experience with Fraud Checks

Fraud checks need to be balanced with customer experience to maintain customer satisfaction and trust. By ensuring that verification processes are user-friendly, communication is transparent, and authentication methods are adaptive, businesses can maintain robust security without disrupting the customer journey.

The fraud prevention measures listed above must be deeply integrated into departmental processes and daily user activities so that they operate seamlessly in the background. These measures should be so well-implemented that customers hardly notice them, even while they continue securing the environment.

This approach, in line with the Dynamic Fort Knox concept, allows for a robust operation where strong fraud prevention measures protect the business and its customers without compromising the overall user experience.

Improving Your Fraud Prevention Strategy in Practice

Obviously, no business needs to implement all the strategies above. Moreover, many do not have the bandwidth to support implementation and execution of all these strategies. That is why it is imperative to assess your department's goals and frequent customer profiles to decide which tools and strategies to employ.⁵

Your Fort Knox does not have to be enormous, but it must be agile. It should effortlessly identify and address all potential threats, while delivering an exceptional experience to your department and customers.

This is why partnering with vendors who thoroughly understand your business and can help you build your own Fort Knox is crucial. Vendors need to solve your particular needs, which is why custom solutions as opposed to out-of-the-box products are vital.

Conclusion

The particulars for building a Dynamic Fort Knox covered in this article are based on what we know now. The field is constantly changing, however, and tools used today may not be the same ones used tomorrow.

That's why it's crucial that your fraud fortress is dynamic and tailored to your business. More important than including everything is studying what works for you and only implementing what's necessary. Customer experience is key, and unnecessary pieces to your operation only make it worse.

There's no one-size-fits-all solution to fraud. Studying your organization's needs and customer profiles is at the core of the Dynamic Fort Knox concept, more than any set of tools. When you implement such a tailored and dynamic system, you will be capable of taking on fraud now and into the future, whatever changes come.

About the authors:

Ali Kidwai is the Product & Implementation Manager at Bectran, where he develops value-driven products and forges strategic partnerships to address challenges in the order-to-cash industry. His expertise spans payments, accounts receivable, claims, and collections. Over the

⁵ This approach fits with the ACFE's recommendation in its 2024 report. They find that the most effective fraud strategies set appropriate priorities, specifically for rapid detection and cost reduction.

past six years, Ali has collaborated with industry leaders in building materials and distribution, food and beverage, chemicals, and manufacturing.

Ali holds a Bachelor's degree in Finance and a Master's in Information Systems from Indiana University's Kelley School of Business. His background equips him to offer forward-thinking advice on the future of finance and treasury. Furthermore, Ali has successfully led over 50 digital transformation projects, including many with Fortune 500 companies, delivering innovative solutions that respond to client insights and needs.

Lilly Filippov brings over a decade's expertise to her role as Senior Marketing Manager at Bectran. She developed her craft working closely with technical and product development teams, making her adept at grasping client and industry challenges and responding with strategic, high-impact marketing initiatives. Lilly holds a bachelor's in Marketing from DePaul University and offers continuous creative solutions for elevating product and brand positioning.

Nathaniel Stickman is a content and copywriter whose technical background makes him especially suited to understanding complex problems and conveying solutions simply. With a master's in English Literature and over a decade writing, editing, and managing corporate knowledge, Nathaniel offers a clear and comprehensive perspective when it comes to written content.

Non Profit Org.
U.S. Postage
PAID
Westminster, MD
Permit No. 855



**Credit Research
Foundation**

1812 Baltimore Blvd, Suite H, Westminster, MD 21157

www.crfonline.org