August 2024

Upping Your Game: Leveraging Red Team Testing and Benchmarking

Jim Mortensen

This report provided compliments of:

GreenwaySolutions

August 2024

Upping Your Game: Leveraging Red Team Testing and Benchmarking

Jim Mortensen

Table of Contents

List of Figures

List of Tables

Summary and Key Findings

As fraudsters employ increasingly sophisticated tactics and financial institutions (FIs) continually upgrade and expand their products and services, FIs must adopt proactive approaches to identify vulnerabilities, assess their controls' effectiveness, and compare their practices against industry peers. Analyzing anonymized data provided by Greenway Solutions, the creators of Fraud Red Team risk assessment, offers valuable insights into current fraud prevention practices, emerging trends, and the value of red team testing and benchmarking. The key findings from this report follow:

- **Testing vs. benchmarking:** Regular, independent benchmarking and Fraud Red Team testing are essential components of a robust fraud prevention framework, offering benefits beyond competitive analysis to enhance operational resilience and regulatory compliance.
- **Independent testing:** Using an independent red team approach to test fraud controls provides a crucial element to uncover vulnerabilities by simulating real-world scenarios across multiple channels and customer life cycle stages.
- **New account opening:** Account opening processes vary significantly among FIs, particularly in identity verification methods and the validation of customer-provided information such as email addresses and phone numbers. Moreover, new account funding and funds availability policies show considerable variation across institutions, with some banks offering much higher initial deposit limits and faster availability.
- **Authentication and detection:** Authentication controls for account access differ widely among banks, with varying adoption of advanced techniques like biometric authentication and behavioral analytics. Detection controls for fraudulent account maintenance and money movement transactions vary based on different algorithms and the need to maintain the balance between fraud detection and customer friction.

These findings underscore the complex and evolving nature of fraud prevention in the financial services industry. By leveraging comprehensive testing and benchmarking strategies, FIs can improve their defenses against fraudulent activities while also enhancing the customer experience. The insights provided in this report aim to guide FIs in developing more effective, adaptive, and customer-centric fraud prevention strategies.

Introduction

Red team testing and benchmarking are quickly gaining prominence within many fraud prevention strategies. In the evolving landscape of financial transactions and digital interactions, the need for robust fraud prevention measures has never been more critical. As organizations strive to protect their assets and maintain the trust of their customers, FIs increasingly turn to testing their fraud controls in the same way they examine cybersecurity controls—through rigorous red team testing, which involves simulating real-world attacks to identify and understand vulnerabilities in an organization's defenses, typically by a third party. This proactive approach helps organizations improve their security posture by uncovering and addressing weaknesses before malicious actors can exploit them.

The intersection of red team testing and benchmarking in fraud prevention represents a strategic opportunity for organizations to leverage external tools and data sets and more effectively combat the ever-evolving tactics employed by fraudsters. As the digital landscape expands, so do the challenges associated with securing sensitive information. By exploiting the synergies between red team testing and benchmarking, organizations can elevate their defenses against fraud, foster a culture of continual improvement, and navigate the complex landscape of financial security with resilience and confidence. The insights provided in this report aim to guide FIs in developing more effective, adaptive, and customer-centric fraud prevention strategies in an increasingly digital and interconnected financial landscape.

Methodology

This report leverages anonymized data and analysis provided to Datos Insights by Greenway Solutions, also known as the Fraud Red Team, offering insights into the challenges faced by financial services firms in the rapidly evolving fraud landscape. The findings are further augmented by Datos Insights' comprehensive ongoing research on fraud trends within the industry, which includes quantitative and qualitative studies involving financial services firms and vendors, providing a robust understanding of the current state of fraud threats and related industry tactics.

Improving Fraud Defenses

In the rapidly evolving world of financial services, effective fraud prevention is now critical for institutions to protect their customers as well as their profitability. As fraudsters grow increasingly sophisticated in their methods—employing cutting-edge technologies and exploiting vulnerabilities across multiple products, channels, and life cycle phases—the need for robust, adaptive fraud prevention controls has never been more pressing. However, implementing effective controls is only half the battle; ensuring ongoing control efficacy requires a comprehensive strategy that encompasses rigorous testing and continual benchmarking against industry peers.

The distinction between testing and benchmarking is crucial to understanding their respective roles in a comprehensive fraud prevention strategy. Testing refers to the process of actively assessing the performance of fraud controls within a specific institution, using real-world scenarios and simulated attacks to identify weaknesses and gaps in coverage. By contrast, benchmarking involves comparing an institution's fraud prevention practices and performance against those of its peers, providing valuable insights into industry norms and best practices. These are further defined herein:

- **Testing:** Testing serves as a diagnostic tool to evaluate the strength and efficacy of existing controls through systemic examination of internal processes, access controls, and transaction monitoring systems. By examining test results and related evidence, organizations can detect and analyze vulnerabilities proactively as opposed to waiting for them to be exposed by fraudsters. A detailed assessment helps in identifying potential weaknesses and allows organizations to proactively fortify their fraud defenses.

- **Benchmarking:** By introducing a comparative dimension to evaluating fraud prevention strategies, benchmarking assesses an organization's controls against industry practices and those of peers and helps to gauge the effectiveness of current measures while understanding competitive practices. By doing so, organizations can identify areas needing improvement and provide valuable insights for enhancing fraud prevention efforts.

Red team testing can further advance an effective fraud prevention system by having rigorous testing performed by an independent third party. While organizations test controls when implemented, a frequently missing component involves the inclusion of independent red team testing, which provides a whole new dimension to an organization's level of assurance. Cybersecurity professionals have leveraged red team testing through independent consultants for years through penetration (pen) testing; this has grown to be a mandatory component of cybersecurity controls at FIs. The extension of this concept to fraud prevention is a natural evolution, given the importance of maintaining security over customer data and preventing losses.

Both red team testing and benchmarking are quickly becoming critical to fully understand, assess, and refine the broader control landscape. Red team testing provides a detailed, independent evaluation of an FI's specific fraud prevention controls while benchmarking compares these measures against industry standards and best practices. This comprehensive approach ensures that all aspects of the institution's controls are assessed, enabling a thorough evaluation of the effectiveness of an FI's defenses. The results often provide internal stakeholders with critical evidentiary information to support remediation efforts and investment requests.

Red Team Testing: Proactively Uncovering Control Vulnerabilities

As fraudsters relentlessly adapt their methods to exploit new vulnerabilities, previously effective controls can swiftly become obsolete or compromised. Thorough testing is crucial to preserving the effectiveness of fraud prevention controls over time. The value of testing extends beyond the immediate identification of control weaknesses. By providing a continuous feedback loop between testers and control designers, testing helps foster a culture of continual improvement and adaptability within fraud prevention teams. This allows them to identify gaps in coverage, fine-tune detection algorithms, and implement additional layers of security where needed. As new vulnerabilities are identified and addressed, the overall resilience of the institution's fraud defenses is strengthened over time:

- Frequent testing enables institutions to stay ahead of evolving threats by proactively identifying weaknesses with testing evidence before they can be exploited.

- The most impactful testing approaches replicate real-world fraud scenarios across products, channels, and phases of the customer life cycle. This becomes most effective when it involves using test accounts that emulate the behavior of legitimate customers and fraudsters and exposing them to a range of scenarios designed to uncover vulnerabilities. For instance, testers may attempt to open accounts using stolen or synthetic identities, capitalize on weaknesses in authentication protocols to gain unauthorized access, or employ social engineering tactics to manipulate customer service representatives.

- Crucially, effective testing requires a degree of independence from the teams responsible for designing and implementing fraud controls. This helps to ensure an objective assessment of control performance and avoid the risk of blind spots or biases that can arise when controls are evaluated by those who created them.

Many institutions choose to engage third-party testing services or establish dedicated red teams to provide an independent perspective. By executing test cases that encompass the full range of potential attack vectors—from identity theft and account takeover to payment fraud and location spoofing—FIs can gain a comprehensive understanding of their fraud prevention controls’ strengths and weaknesses.

Benchmarking: Learning From Industry Peers

While testing focuses on the performance of an individual institution’s fraud controls, benchmarking offers valuable context by comparing these controls to those of industry peers. By understanding how their fraud prevention practices and performance measure up against similar institutions, organizations can pinpoint areas in which they may be falling behind or excelling relative to industry norms. Benchmarking can encompass a wide range of metrics and practices, from the specific technologies and detection methods used to the organizational structures, customer limits, and tools that support fraud prevention efforts.

One of the key challenges of benchmarking is obtaining reliable and comparable data from peer institutions. While some high-level benchmarking data may be available through industry associations or research firms, more detailed comparisons often require direct collaboration between institutions. For example, an institution may seek to benchmark its false positive rates for transaction monitoring, its average detection times for different types of fraud, or the level of investment it makes in fraud prevention staffing and training. This can raise concerns about data privacy and competitive dynamics, which must be carefully managed through appropriate data-sharing agreements and governance structures.

Despite these challenges, the insights gained from benchmarking can be invaluable in guiding an institution’s fraud prevention strategy. By identifying areas in which they are underperforming relative to peers, institutions can prioritize investments and improvements that will have the greatest impact on their overall fraud defenses.

Conversely, areas in which an institution is outperforming its peers can provide valuable best practices that can be shared more broadly across the industry.

Developing a Comprehensive Testing and Benchmarking Strategy

To fully realize the benefits of testing and benchmarking, institutions must develop comprehensive testing and benchmarking strategies that integrate into their overall fraud prevention efforts and policy development. This strategy should be tailored to the unique risks and challenges faced by the institution, considering factors such as its size, customer base, product offerings, and geographic footprint. These are some key elements of a comprehensive testing and benchmarking strategy:

- Independent testing teams or third-party services to ensure objective assessments
- A robust inventory of real funded accounts across a broad range of FIs
- Regular, proactive testing of fraud controls across all channels and stages of the customer life cycle
- Collaboration with industry peers to establish benchmarking data and best practices
- Integration of testing and benchmarking insights into fraud prevention planning and prioritization
- Continual monitoring and adjustment of testing and benchmarking approaches to keep pace with evolving threats and industry trends

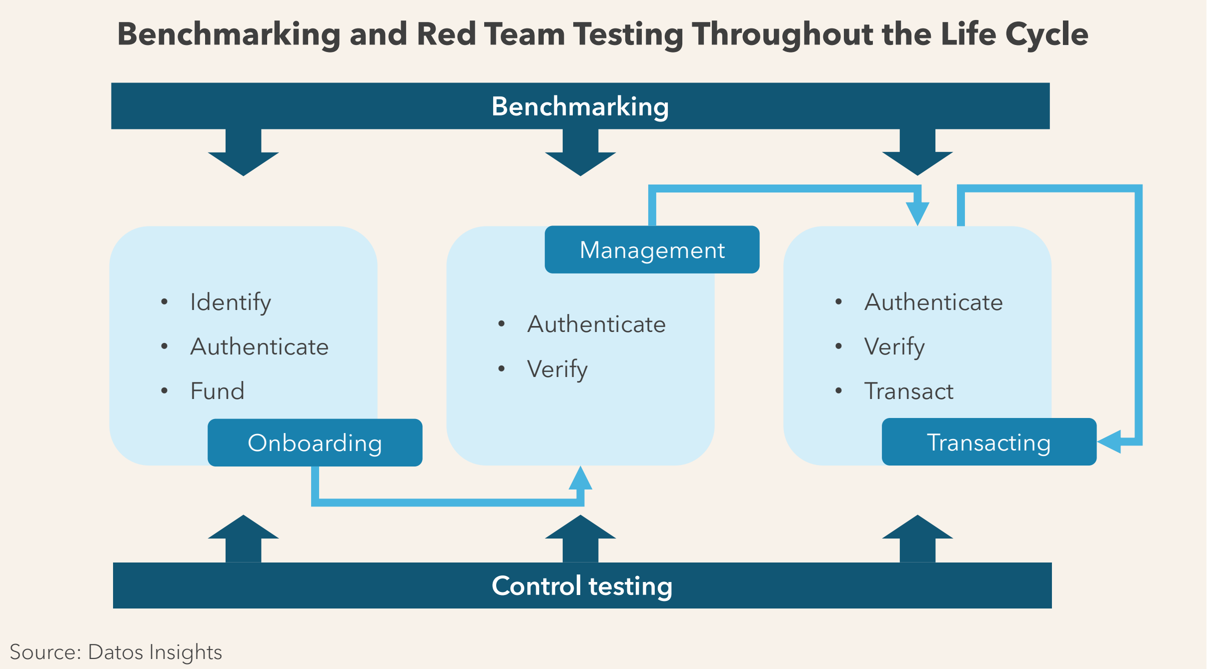
Moreover, the testing and benchmarking strategy should consider the full customer life cycle— from onboarding to transacting—and the related control points (Figure 1).

- **Onboarding:** Tests should be designed that address the key controls when customers are onboarded, including the validation of the identity, the verification of any linked accounts, and the validation of key data elements such as the email address, phone number, and related Social Security number.
- **Management:** Once the account is on the books, the biggest risk is that it is taken over by a fraudster and drained of any funds or credits that are available. Developing a high level of assurance that customers won't be broadly compromised requires constructing tests and performing benchmarking that provide high levels of assurance that the FI's

authentication and verification processes are effective, customer-friendly, and competitive.

- **Transacting:** Finally, a strong control framework that ensures that the authentic consumer is transacting and addresses all types of payment mechanisms is central to fraud prevention. Control tests tailored to each transaction type are an essential element.

Figure 1: Benchmarking and Red Team Testing Throughout the Life Cycle



Source: Datos Insights

This holistic approach ensures that fraud prevention measures are not only robust at individual stages but also coherent and adaptive throughout the customer journey. Moreover, it allows institutions to strike an optimal balance between security and customer experience at each phase, fostering trust and loyalty while effectively mitigating fraud risks.

Benchmarking and Testing Across the Customer Life Cycle

Effective policy and process benchmarking and testing are essential to optimize fraud prevention efforts. By testing and comparing institutional policies and processes to those of industry peers throughout the customer life cycle, organizations can identify areas in which they may be lagging or excelling. Performing genuine red team-type testing can give the institution confidence that policies and processes are functioning as designed and are truly effective.

Onboarding Customers

The account opening process represents a critical juncture in the customer journey, as it serves as the first line of defense against fraudulent activity. Criminals often exploit vulnerabilities in this stage to create fake accounts using stolen or synthetic identities, laying the groundwork for future financial crimes. By benchmarking their account opening procedures against those of their peers, FIs can gain valuable insights into industry-leading practices and identify potential weaknesses in their controls.

This comparative analysis may encompass a range of measures, including the types of identity documents accepted, the use of identity verification services, and the application of advanced technologies such as biometrics or machine learning algorithms to detect anomalies or inconsistencies in applicant data. In addition to validating core customer identity elements, such as name, address, and date of birth, FIs also recognize the importance of verifying additional information provided during the account opening process, such as email addresses and phone numbers.

While Table A illustrates that FIs are performing the verification, and there is some commonality in the data that is validated and the techniques leveraged, it is not consistent across FIs. An interesting finding is the relatively limited use of the Social Security Administration's (SSA) electronic Consent Based Social Security Number Verification (eCBSV) service. With only two of seven FIs utilizing eCBSV, as shown in Table A, this capability, which was viewed as an opportunity to validate identity credentials at the issuing source (the SSA), does not appear to be employed to the extent originally envisioned.

Table A: Account Opening Comparison

Verification performed	Tier-1 banks	Fintech firms	Online banks	All FIs
Email confirmed	3 of 5	0 of 1	0 of 1	3 of 7
Email validated	3 of 5	0 of 1	0 of 1	3 of 7
Phone validated	4 of 5	1 of 1	1 of 1	6 of 7
eCBSV requested	2 of 5	0 of 1	0 of 1	2 of 7
Knowledge-based authentication (KBA)	3 of 5	0 of 1	0 of 1	3 of 7

Source: Greenway Solutions, Q1 2022

By comparing their validation techniques to those employed by other institutions, FIs can stay abreast of emerging threats and adapt their controls accordingly to ensure a more secure and resilient account opening process.

New Account Funding

New account funding and funds availability testing play a vital role in assessing the robustness of an FI's fraud prevention controls when onboarding an account or new relationship. By simulating various funding scenarios, such as initial deposits, transfers from external accounts, and mobile remote deposit capture (MRDC), testing can evaluate the effectiveness of the institution's risk assessment processes, transaction monitoring systems, and funds availability policies.

As shown in Table B, an analysis of funds availability testing reveals a wide range of policies across FIs, with some banks providing a high level of availability on the initial deposit and more restrictive availability on subsequent deposits.

Table B: New Account Funding, Funds Availability Testing

	Initial funding		Deposit 1		Deposit 2		Deposit 3	
Bank	Days	Available	Days	Available	Days	Available	Days	Available
Tier-1 bank	1	67%	1	17%	0	60%	0	89%
Tier-1 bank	7	100%	1	19%	1	100%	0	100%
Tier-1 bank	4	100%	6	100%	1	100%	0	100%
Tier-1 bank	11	100%	3	100%	11	100%	0	18%
Online bank	0	100%	0	25%	0	60%	0	54%
Fintech	1	100%	0	63%	0	19%	0	40%

Source: Greenway Solutions, Q1 2022

New account funding policies and processes are often the first key decisions affecting new customers post-approval. This critical juncture can set the tone for the entire customer relationship, and it presents a unique set of risks and opportunities. By comparing institutional practices to those of industry peers, FIs are better able to strike an optimal balance between effecting strong risk management and delivering a superior customer experience:

- Effective benchmarking enables institutions to assess whether initial deposit limits, funds availability time frames, and verification procedures are competitive as compared to the industry while still providing adequate fraud protection.
- It may help to identify new and innovative approaches to streamline the onboarding process, potentially reducing unnecessary friction for new customers without compromising security.

Managing Accounts

Account access and authentication controls serve as critical safeguards against unauthorized access to customer accounts, particularly in an era of increasing digital interactions and reliance on online and mobile banking platforms. FIs must implement robust, multilayered authentication protocols that optimize security and user experience, ensuring that legitimate customers can easily access their accounts while also preventing fraudsters from gaining entry. Doing so may involve the use of traditional methods such as passwords and one-time passcodes (OTPs) or more advanced techniques like biometric authentication, behavioral analytics, and behavioral biometrics based on the user's risk profile and transaction history.

Benchmarking authentication controls and practices against those of peers enables institutions to gain deeper insights into industry-leading practices and to identify and address potential weaknesses or gaps in their security measures.

Online Authentication Controls

Leading fraud control testing practices should integrate an assessment of the resilience of authentication controls in the face of common customer behaviors, such as poor password hygiene, the use of multiple devices, as well as the institution's ability to support secure account recovery and password reset processes. Additionally, an evaluation of an FI's policies and processes covering the secure access of systems by customers should include an understanding of the tools provided for customers, such as a password strength indicator on the app or website, the ability to control the options for two-factor authentication (2FA) and the ability for the customers to view and manage the devices accessing their accounts.

As shown in Table C, significant differences exist in the breadth of authentical controls adopted across the different types of FIs. Knowing how an FI compares to its peer group can help guide the functionality provided to customers to stay secure while remaining competitive.

Table C: Online Authentication Controls

Control feature	Tier-1 banks	Tier-2 banks	Online banks	All FIs
Password strength indicator	1 of 6	2 of 3	2 of 3	5 of 12
Fast login option	1 of 6	1 of 3	1 of 3	3 of 12

Control feature	Tier-1 banks	Tier-2 banks	Online banks	All FIs
View and manage devices	4 of 6	1 of 3	0 of 3	5 of 12
Control of 2FA options	5 of 6	1 of 3	2 of 3	8 of 12
Card controls	1 of 6	1 of 3	1 of 3	3 of 12
Channel controls	2 of 6	1 of 3	2 of 3	5 of 12

Source: Greenway Solutions, Q3 2023

The differences among firms also expose certain less common and emerging features that an FI may want to consider including in its arsenal of capabilities:

- **Fast login option:** The ability for customers to execute a fast, secure login through short PINs wherein the device is trusted based upon some combination of device intelligence or behavioral biometrics
- **Card controls:** The ability for customers to turn their debit or credit cards on and off to control their use better and protect against fraudulent charges
- **Channel controls:** The ability for customers to control which channels they (or authorized users on their account) can use, such as telephone banking

Authentication Practices

A comprehensive fraud control testing program should drill down a bit deeper into the policies employed for certain key controls. For example, an OTP control framework will include elements such as the expiration time for an issued OTP and the specific circumstances when an OTP is required. While institutions will require an OTP when a new or unrecognized device is detected, other practices and protocols can vary greatly from one firm to the next, as shown in Table D.

Table D: Step-Up OTP Authentication Practices

Bank type	Expiration time frame	Customer option for OTP	New or unknown device	Required each login	OTP contact options
Tier-1 bank	10 minutes	□	■	□	V, T, E

Bank type	Expiration time frame	Customer option for OTP	New or unknown device	Required each login	OTP contact options
Tier-1 bank	None	■	■	□	V, T, M, O
Tier-1 bank	None	■	■	□	V, T, E, O
Tier-1 bank	None	■	■	□	V, T, M, E, O
Tier-1 bank	10 to 20 minutes	□	■	□	V, T
Tier-1 bank	5 minutes	□	■	□	V, T
Tier-2 bank	None	■	■	■	T, O
Tier-2 bank	None	□	■	□	V, T
Online bank	20 minutes	□	■	□	V, T
Online bank	None	□	■	□	V, T
Online bank	None	□	■	□	V, T
Online bank	None	□	■	□	T, E

Source: Greenway Solutions, Q4 2023 Key: V = Voice phone call, T = SMS text, M = Mobile app push, E = Email, O = Token and other

Some institutions provide customers with the ability to require an OTP for their username each time a login is attempted, thus increasing the level of security on their accounts. Also, despite the fact that SMS text is subject to compromise, it is the most common option offered, while mobile app push is one of the least common options available. By comparing their authentication methods and practices, institutions can identify areas for improvement and innovative approaches to enhance security. Rigorous testing of these controls, particularly through simulated attack scenarios, helps uncover vulnerabilities and assess the real-world effectiveness of authentication measures.

Facilitating Customer Transactions

Thorough testing and benchmarking of transaction management controls can help to ensure effectiveness in mitigating fraud risk across a wide range of scenarios. This testing should encompass both normal customer behavior and simulated fraudulent activity, such as attempts to cash fraudulent checks, initiate unauthorized wire transfers, or exploit vulnerabilities in account-to-account transfer processes. By regularly testing and refining their transaction management controls, FIs can provide a more secure and efficient transaction processing environment, reducing the risk of financial losses and reputational damage while ensuring a seamless customer experience.

Check Cashing

Understanding how an FI's transaction controls compare to its peer group and others that perform the same service can uncover opportunities to shore up controls while also helping to ensure its processes are competitive or in line with the industry.

Table E provides an analysis of various bank and retailer policies around the acceptance of third-party checks and the information requirements. The table also shows an acceptance test that was performed and the related results.

Table E: Check-Cashing Policy and Controls

Type of business	Driver license review	Driver license scan	Multiple IDs required	Check amount (in US$)	Stolen/ forged	Decision
Tier-1 bank	Yes	No	No	$110	No	Accepted
Tier-1 bank	No	No	Yes: passport, bank card	$110	No	Accepted
Tier-2 bank	Yes	No	Yes: government ID, bank card	$110	No	Accepted
Tier-1 bank	Yes	No	Yes: multiple options	$110	Yes	Accepted
Retail/grocery store	Yes	Yes	No	$106	No	Denied
Retail/grocery store	Yes	Yes	No	$105	No	N/A
Convenience store	Yes	Yes	No	$105	Yes	N/A

Type of business	Driver license review	Driver license scan	Multiple IDs required	Check amount (in US$)	Stolen/ forged	Decision
Check-cashing store	Yes	Yes	Yes: passport	$105	No	N/A

Source: Greenway Solutions, February 2023

Interestingly, retail establishment policies were more stringent than those banks included in the analysis. This type of information can be key for institutions to evaluate their policies and determine how to be more competitive while controlling for the significant risk around cashing checks.

Wire Transfers

Wire transfers are a critical service offered by FIs that enable customers to move funds quickly and securely between accounts, often with a sense of urgency driven by time-sensitive transactions or pressing financial obligations. However, the speed and irrevocability of wire transfers also make them an attractive target for fraudsters, who may attempt to exploit vulnerabilities in the wire transfer process to initiate unauthorized transactions or intercept legitimate ones. To mitigate these risks, institutions establish robust controls around wire transfer initiation, approval, and execution processes, including multi-factor authentication, dual control procedures, and real-time monitoring for suspicious activity.

Benchmarking wire transfer controls against peers provides institutions valuable insights into industry-leading practices and identifies opportunities to streamline processes without compromising security. Armed with this competitive intelligence, institutions can make informed decisions about how to optimize their wire transfer controls.

Table F demonstrates the controls across banks at various steps within the wire transfer process, from login through the sending of the wire, and the variation in control techniques within each step.

Table F: Online Wire Transfer Controls for a US$1,000 Transfer

Process step	Control tool	Tier-1 bank	Tier-1 bank	Tier-1 bank	Tier-1 bank	Tier-1 bank	Online bank
Login	User ID/ password	✓	✓	✓	✓	✓	✓
Wire access	OTP			✓			
Add recipient	OTP				✓		
	Verify owner				✓		
	Email alert	✓	✓				
Send wire	OTP	✓	✓			✓	
	Debit card PIN			✓			
	Debit speed	■	◩	◩	■	◩	■
	Daily limit	$25,000	$25,000	Balance	Balance	$25,000	Balance
Wire sent alert	Push notification	✓					
	Email	✓	✓	✓	✓		
	Text			✓			
Wire received alert				✓			
Inbound funds available	Credit Speed	◩	✗	■	□	◩	■

Source: Greenway Solutions, March 2022; Key: ▯ = Yes, ■ = Immediate, ◩ = 1 to 2 hours, □ = End of day, ▯ = Multiple days

From the analysis, it is evident that a wide range of control types are utilized across organizations, with some lacking certain controls. In particular, the online bank in the study had very few hurdles coupled with fast debiting of the account, which could result in higher fraud loss rates.

MRDC

Benchmarking and testing MRDC controls for new accounts are crucial for FIs to understand industry standards, assess their risk appetite, and optimize the balance between fraud prevention and customer experience in the early stage of the relationship. By comparing their practices to those of peers, banks can identify potential gaps in their controls and uncover leading practices. Moreover, organizations can make informed decisions about deposit limits and funds availability policies that are particularly important for new or low-tenured accounts, as MRDC processes are often targets for fraudsters and require careful risk management.

Table G highlights several insightful findings that emerged from a benchmarking exercise on MRDC practices across different institutions. For instance, the time taken for initial deposits to become fully available varies significantly, ranging from five to 11 days across different institutions.

Table G: MDRC for New Accounts

FI type	Deposit limit (US$ per day/ month)	Fund availability	Additional findings
Tier-1 bank	$5,000/$10,000	• Same day: Yes, at 30 days • Next day: Percentage • Remainder: Percentage	• Initial deposit took five days • Availability varies by account age, amount, and maker bank
Tier-1 bank	$25,000/$50,000	• Same day: No • Next day: Up to 100% • Remainder: Percentage	• Initial deposit took seven days • After 30 days, availability is next day
Tier-1 bank	Unspecified	• Same day: No • Next day: Percentage • Remainder: Up to six days	• Initial deposit took nine days • Availability limit increased to US$15,000 on day 90

FI type	Deposit limit (US$ per day/ month)	Fund availability	Additional findings
Tier-1 bank	$5,000/$20,000	• Same day: Yes, at 60 days • Next day: Percentage • Remainder: Up to 11 days	• Initial deposit took 11 days to become fully available
Tier-1 bank	Not tested	• Not tested	• MRDC unavailable for 180 days
Online bank	$50,000/$250,000	• Same day: No • Next day: Up to $300 • Remainder: Two to four days	• Initial deposit was next day • Consistently delays a large percentage for two to four days
Fintech	$5,000/$10,000	• Same day: No • Next day: Up to $225 • Remainder: 14 days	• Must be signed up for direct deposit

Source: Greenway Solutions, April 2022

This wide disparity indicates that banks are particularly cautious with the first MRDC deposit from a new account. Similarly, some institutions impose waiting periods before allowing MRDC usage, with one Tier-1 bank not permitting MRDC for the first 180 days of an account's life. These practices underscore the heightened risk associated with new accounts and the need for robust controls during the early stages of the customer relationship.

It is highly advised that institutions test and benchmark MRDC controls for tenured accounts separately from new or low-tenure accounts, as established customers typically anticipate more favorable treatment, such as higher deposit limits and quicker access to funds, as a result of their longstanding relationship with the FI. By comparing MRDC policies for tenured accounts against industry peers, banks are better able to meet these higher customer expectations without degrading risk controls. FIs can strike the right balance between customer satisfaction and fraud prevention for their most loyal clientele.

Several insights can be gleaned from this sort of benchmarking study separate from new or low-tenure accounts, as shown in Table H:

- Some banks maintain consistent policies between new and tenured accounts, while others significantly increase limits and improve availability for longstanding customers. This may suggest that banks elect to deploy different approaches to rewarding customer loyalty and managing risk over different periods.
- The highest monthly limit of US$1.5 million, offered by an online bank, stands out as an outlier and may indicate an organizational business strategy to attract high-value customers.
- The discrepancy noted in one Tier-1 bank's communication about same-day availability vs. the actual next-day availability highlights the importance of clear and accurate customer communication.

Table H: MDRC for Tenured Accounts

Bank type	Deposit limit (US$ per day/ month)	Fund availability	Additional findings
Tier-1 bank	Unclear/$15,000	• Same day: No • Next day: 100%	• No daily limit observed • Next business day availability unless a hold is placed
Tier-1 bank	$50,000/$50,000	• Same day: Depends • Next day: 100%	• Same-day fund availability range varies based on amount and maker bank
Tier-1 bank	$5,000/$10,000	• Same day: No • Next day: 100%	• Noted difference in limits for the new and tenured accounts • Availability policy is consistent for new and tenured accounts
Tier-1 bank	$15,000/$15,000	• Same day: No • Next day: 100%	• Availability policy was consistent for deposits of US$1,000 and US$10,000

Bank type	Deposit limit (US$ per day/ month)	Fund availability	Additional findings
Tier-1 bank	$7,500/$15,000	• Same day: No • Next day: 100%	• Bank verbiage says US$500 is available immediately, but the reality is funds are available next day
Tier-1 bank	$25,000/$150,000	• Did not test	• Checked limits for tenured, high-balance accounts
Online bank	$50,000/ $1.5 million	• Same day: No • Next day: Up to $300 • Remainder: Two to four days	• Highest monthly limit • Availability policy is consistent for new and tenured accounts
Online bank	$25,000/$50,000	• Same day: Up to $250 • Next day: None	• Remainder of up to US$5,300 is available by day four; the rest is available by day seven

Source: Greenway Solutions, April 2022

These findings underscore the need for banks to carefully consider how they balance risk management, customer expectations, and competitive positioning when setting MRDC policies for tenured accounts.

Conclusion

Confronted with ever-evolving fraud threats, constant system upgrades, new products and services, and expanding delivery channels, FIs have a large attack surface to defend. By adopting a strategy that combines rigorous testing with ongoing benchmarking against industry peers, FIs can take steps to proactively identify and address control gaps, prioritize investments for maximum impact, and stay one step ahead of fraudsters:

- Enhance fraud prevention process and policy through rigorous testing and benchmarking to stay ahead of increasingly sophisticated fraudsters and emerging threats.
- Introduce independent red team testing, similar to cybersecurity pen testing, to add a valuable new dimension to fraud control assurance that many organizations currently lack.
- Leverage peer benchmarking to gain insights into best practices, competitive positioning, and areas for improvement in fraud prevention strategies. This is particularly important for critical processes such as account opening and new account funding.
- Understand variations in fraud prevention practices across institutions and develop tailored approaches that balance risk management with customer experience and operational efficiency.
- Regularly evaluate and refine fraud prevention controls, informed by both testing and benchmarking data, to adapt to evolving threats and changing customer behaviors across various transaction types.
- Integrate testing and benchmarking insights into fraud prevention planning and policy development to create a more robust and adaptive risk management strategy that evolves with the threat landscape.

By fostering a culture of continual improvement and adaptation, FIs can not only mitigate fraud risks but also enhance their overall operational resilience and competitive advantage. As the financial services industry continues to transform, the ability to leverage insights from testing and benchmarking will be a key differentiator in building robust, effective, and customer-friendly fraud prevention systems.

About Greenway Solutions

Greenway Solutions is a fraud prevention services firm that has been in business since 2004. Its clients include national banks, regional banks, credit unions, and fintechs in the U.S., U.K., and Canada. It provides its clients with fraud strategy consulting, fraud control assessments, red team testing, implementation services, and data analytics. The breadth of its consulting and testing spans the customer life cycle, including new client acquisition, identity verification, authentication, account maintenance, and all forms of money movement. Fraud Red Team is a turnkey testing service offered by Greenway that uses live accounts to evaluate a bank's customer protection measures, find customer vulnerabilities, and identify fraud control gaps across a bank's customer-facing processes and production systems.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

Jim Mortensen

jmortensen@datos-insights.com