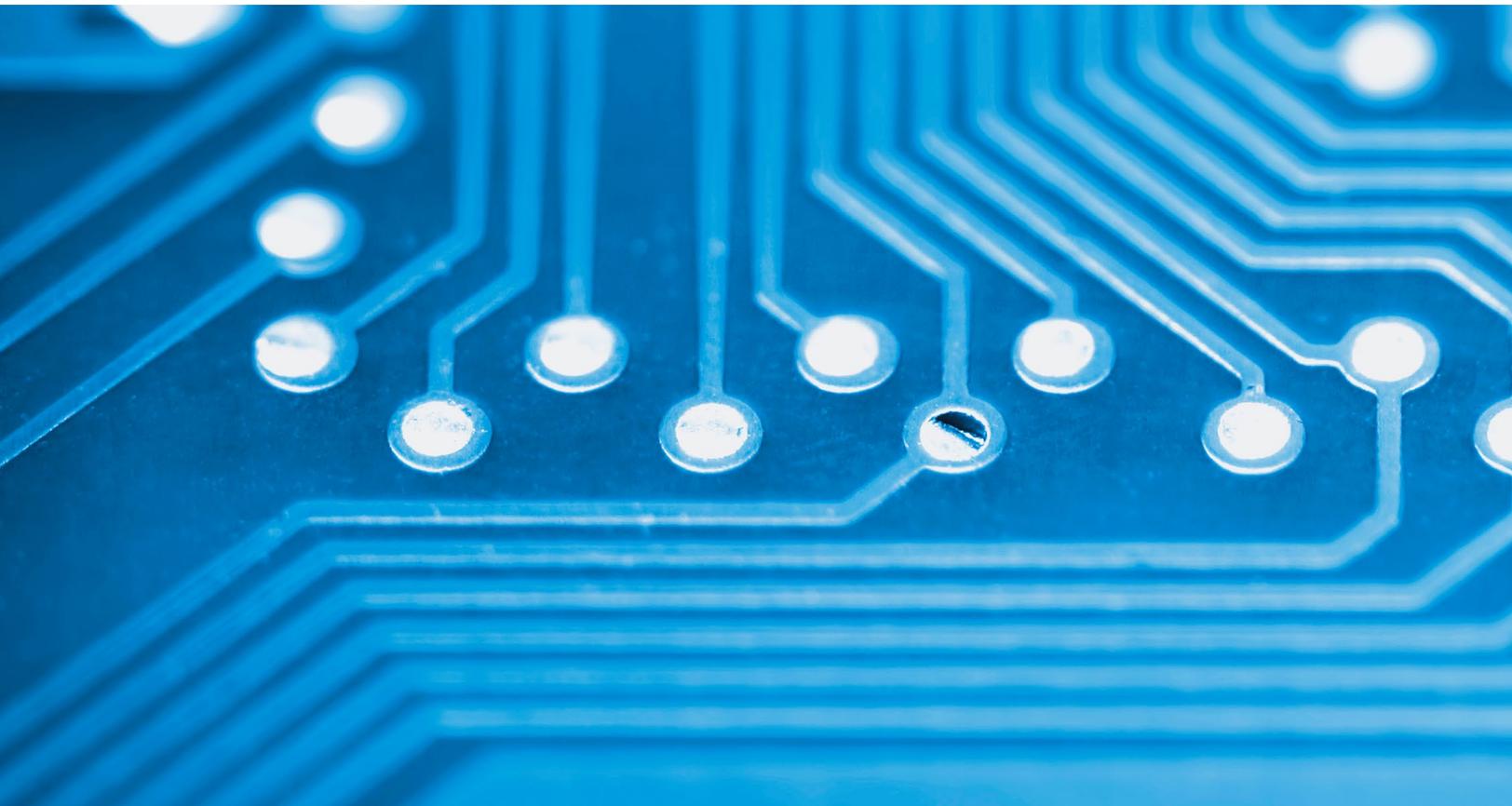


Risk Practice

Financial crime and fraud in the age of cybersecurity

As cybersecurity threats compound the risks of financial crime and fraud, institutions are crossing functional boundaries to enable collaborative resistance.

by Salim Hasham, Shoan Joshi, and Daniel Mikkelsen



In 2018, the World Economic Forum noted that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately \$8.2 billion on anti-money laundering (AML) controls alone in 2017. The crimes themselves, detected and undetected, have become more numerous and costly than ever. In a widely cited estimate, for every dollar of fraud institutions lose nearly three dollars, once associated costs are added to the fraud loss itself.¹ Risks for banks arise from diverse factors, including vulnerabilities to fraud and financial crime inherent in automation and digitization, massive growth in transaction volumes, and the greater integration of financial systems within countries and internationally. Cybercrime and malicious hacking have also intensified. In the domain of financial crime, meanwhile, regulators continually revise rules, increasingly to account for illegal trafficking and money laundering, and governments have ratcheted up the use of economic sanctions, targeting countries, public and private entities, and even individuals. Institutions are finding that their existing approaches to fighting

such crimes cannot satisfactorily handle the many threats and burdens. For this reason, leaders are transforming their operating models to obtain a holistic view of the evolving landscape of financial crime. This view becomes the starting point of efficient and effective management of fraud risk.

The evolution of fraud and financial crime

Fraud and financial crime adapt to developments in the domains they plunder. (Most financial institutions draw a distinction between these two types of crimes: for a view on the distinction, or lack thereof, see the sidebar “Financial crime or fraud?”) With the advent of digitization and automation of financial systems, these crimes have become more electronically sophisticated and impersonal.

One series of crimes, the so-called Carbanak attacks beginning in 2013, well illustrates the cyber profile of much of present-day financial crime and fraud. These were malware-based bank thefts

¹ World Economic Forum Annual Meeting, Davos-Klosters, Switzerland, January 23–26, 2018; *LexisNexis risk solutions 2018 True Cost of Fraud study*, LexisNexis, August 2018, risk.lexisnexis.com.

Financial crime or fraud?

For purposes of detection, interdiction, and prevention, many institutions draw a distinction between fraud and financial crime. Boundaries are blurring, especially since the rise of cyberthreats, which reveal the extent to which criminal activities have become more complex and interrelated. What’s more, the distinction is not based on law, and regulators sometimes view it as the result of organizational silos. Nevertheless, financial crime has generally meant

money laundering and a few other criminal transgressions, including bribery and tax evasion, involving the use of financial services in support of criminal enterprises. It is most often addressed as a compliance issue, as when financial institutions avert fines with anti-money laundering activities. Fraud, on the other hand, generally designates a host of crimes, such as forgery, credit scams, and insider threats, involving deception of financial personnel or services to commit

theft. Financial institutions have generally approached fraud as a loss problem, lately applying advanced analytics for detection and even real-time interdiction. As the distinction between these three categories of crime have become less relevant, financial institutions need to use many of the same tools to protect assets against all of them.

totaling more than \$1 billion. The attackers, an organized criminal gang, gained access to systems through phishing and then transferred fraudulently inflated balances to their own accounts or programmed ATMs to dispense cash to waiting accomplices (Exhibit 1).

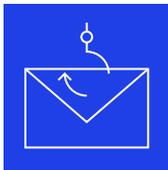
Significantly, this crime was one simultaneous, coordinated attack against many banks. The attackers exhibited a sophisticated knowledge of the cyber environment and likely understood banking processes, controls, and even vulnerabilities arising from siloed organizations and governance. They also made use of several channels, including ATMs, credit and debit cards, and wire transfers. The attacks revealed that meaningful distinctions among cyberattacks, fraud, and financial crime are disappearing. Banks have not yet addressed these new intersections, which transgress the boundary lines most have erected between the types of crimes (Exhibit 2).

A siloed approach to these interconnected risks is becoming increasingly untenable; clearly, the operating model needs to be rethought.

As banks begin to align operations to the shifting profile of financial crime, they confront the deepening connections between cyber breaches and most types of financial crime. The cyber element is not new, exactly. Until recently, for example, most fraud has been transaction based, with criminals exploiting weaknesses in controls. Banks counter such fraud with relatively straightforward, channel-specific, point-based controls. Lately, however, identity-based fraud has become more prevalent, as fraudsters develop applications to exploit natural or synthetic data. Cyber-enabled attacks are becoming more ambitious in scope and omnipresent, eroding the value of personal information and security protections.

Exhibit 1

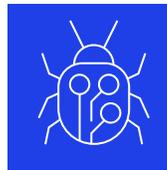
The new cyber profile of fraud and financial crime is well illustrated by the Carbanak attacks.



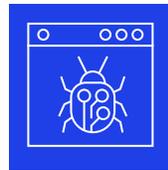
1. Spear phishing
Employee in targeted organization receives email with the Carbanak backdoor as an attachment



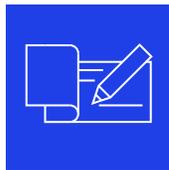
2. Backdoor executed: credentials stolen
Upon opening attachment, employee activates the Carbanak backdoor



3. Machines infected in search for admin PC
Carbanak searches network and finds admin PC; embeds and records



4. Admin PC identified, clerk screens intercepted
Attacker watches admin screen to mimic admin behavior for the bank's cash-transfer systems



5. Balances inflated and inflated amount transferred
Attackers alter balances, pocket extra funds (\$1k account enlarged to \$10k, then \$9k transferred)



6. ATM programmed to dispense cash
Attackers program ATMs to issue cash to waiting accomplices at specific times



7. Cash moved through channels by wire transfers, e-payments
Attackers use online and e-payments to receiver banks to transfer extracted funds

Crime pathways are converging, blurring traditional distinctions among cyber breaches, fraud, and financial crimes.

Fraud and insider threats



- Internal and external threats
- Retail and nonretail threats
- Insider threats
- Market abuse and misbehavior

Cyber breaches



- Confidentiality
- Integrity
- Systems availability

Financial crimes



- Money laundering
- Bribery and corruption
- Tax evasion and tax fraud

Example: cyberattack on a central bank

- Bank employee's SWIFT¹ credentials stolen with the help of insiders
- Malware surreptitiously installed on the bank's computers to prevent discovery of withdrawals
- Funds routed from bank's account at a branch of another country's central bank to a third bank (on a weekend to ensure staff absence)
- Withdrawals were made at the third bank through multiple transactions that were not blocked until too late
- Attacks may have been linked to a known sanctioned entity

¹ Society for Worldwide Interbank Financial Telecommunication.

In a world where customers infrequently contact bank staff but rather interact almost entirely through digital channels, "digital trust" has fast become a significant differentiator of customer experience. Banks that offer a seamless, secure, and speedy digital interface will see a positive impact on revenue, while those that don't will erode value and potentially lose business. Modern banking demands faster risk decisions (such as real-time payments) so banks must strike the right balance between managing fraud and handling authorized transactions instantly.

The growing cost of financial crime and fraud risk has also overshot expectations, pushed upward by several drivers. As banks focus tightly on reducing liabilities and efficiency costs, losses in areas such as customer experience, revenue, reputation, and even regulatory compliance are being missed (Exhibit 3).

Bringing together financial crime, fraud, and cyber operations

At leading institutions the push is on to bring together efforts on financial crime, fraud, and

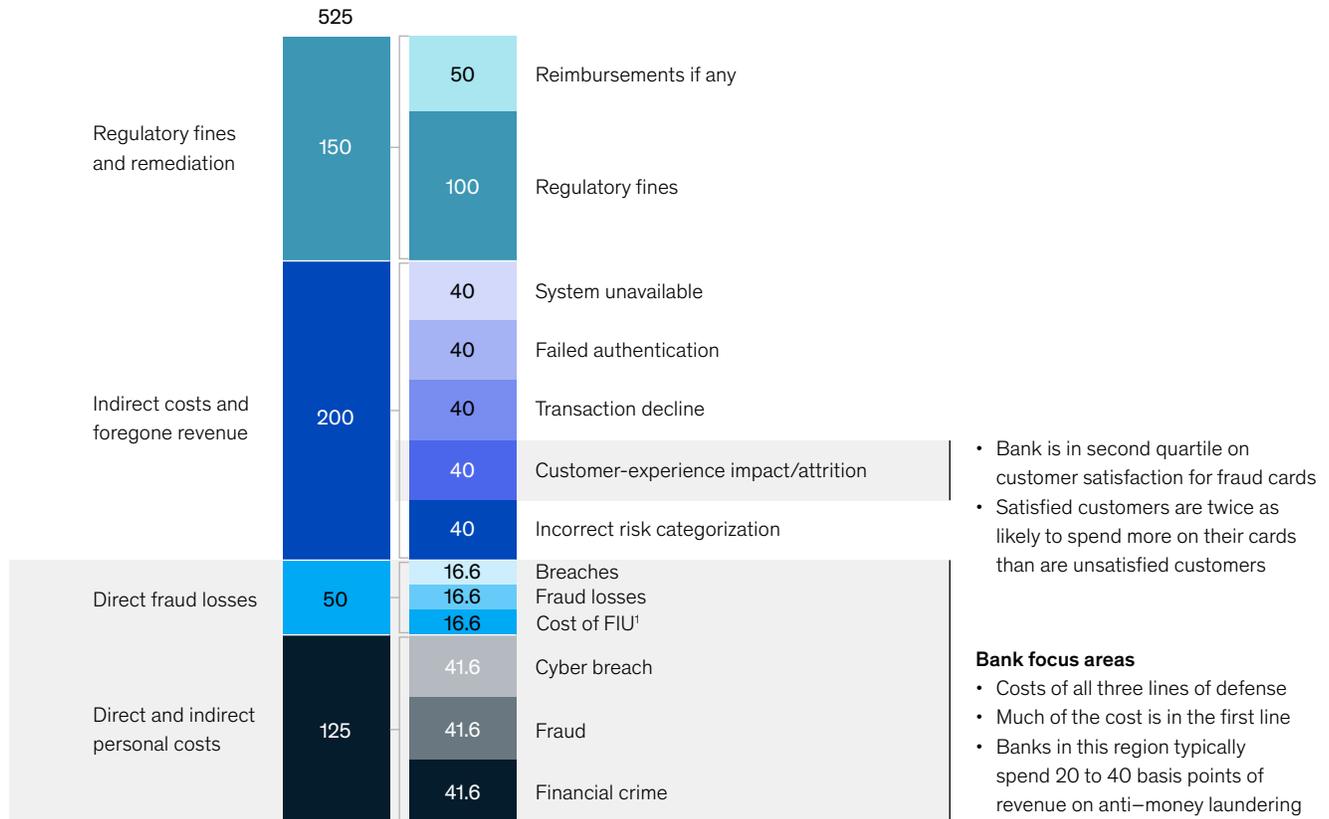
cybercrime. Both the front line and back-office operations are oriented in this direction at many banks. Risk functions and regulators are catching on as well. AML, while now mainly addressed as a regulatory issue, is seen as being on the next horizon for integration. Important initial steps for institutions embarking on an integration effort are to define precisely the nature of all related risk-management activities and to clarify the roles and responsibilities across the lines of defense. These steps will ensure complete, clearly delineated coverage—by the businesses and enterprise functions (first line of defense) and by risk, including financial crime, fraud, and cyber operations (second line)—while eliminating duplication of effort.

All risks associated with financial crime involve three kinds of countermeasures: identifying and authenticating the customer, monitoring and detecting transaction and behavioral anomalies, and responding to mitigate risks and issues. Each of these activities, whether taken in response to fraud, cybersecurity breaches or attacks, or other financial crimes, are supported by many similar data and processes. Indeed, bringing these data sources together with analytics materially

Exhibit 3

Banks often focus on only a fraction of total financial-crime, fraud, and cybersecurity costs.

Example of financial-crime, fraud, and cybersecurity costs, \$ million



¹ Financial intelligence unit.

improves visibility while providing much deeper insight to improve detection capability. In many instances it also enables prevention efforts.

In taking a more holistic view of the underlying processes, banks can streamline business and technology architecture to support a better customer experience, improved risk decision making, and greater cost efficiencies. The organizational structure can then be reconfigured as needed. (Exhibit 4).

From collaboration to holistic unification

Three models for addressing financial crime are important for our discussion. They are distinguished by the degree of integration they represent among processes and operations for the different types of crime (Exhibit 5).

Generally speaking, experience shows that organizational and governance design are the main considerations for the development of the operating model. Whatever the particular choice, institutions will need to bring together the right people in agile teams, taking a more holistic approach to common processes and technologies and doubling down on analytics—potentially creating “fusion centers,” to develop more sophisticated solutions. It is entirely feasible that an institution will begin with the collaborative model and gradually move toward greater integration, depending on design decisions. We have seen many banks identify partial integration as their target state, with a view that full AML integration is an aspiration.

At their core, all functions perform the same three roles using similar data and processes.

	Identification: “Who is my customer?”	Monitoring: “What transactions are legitimate?”	Response: “How do I respond to a threat?”
Financial crime	<ul style="list-style-type: none"> • Client risk rating • Client due diligence; enhanced due diligence 	<ul style="list-style-type: none"> • Transaction monitoring • Name screening • Payments screening 	<ul style="list-style-type: none"> • Suspicious-activity monitoring • Financial intelligence unit • List management • Do not bank
Fraud	<ul style="list-style-type: none"> • Identity verification, including digital and nondigital presence 	<ul style="list-style-type: none"> • Transaction monitoring and decision making • Device and voice analytics 	<ul style="list-style-type: none"> • Investigations and resolutions teams
Cybersecurity	<ul style="list-style-type: none"> • Credentials management 	<ul style="list-style-type: none"> • Security-operations center (SOC) and network-operations center, which enable monitoring 	<ul style="list-style-type: none"> • SOC • Forensics • Resolution teams
Synergies across functions	<ul style="list-style-type: none"> • Risk scoring of customers using common and similar customer data, such as financials, digital footprint, nondigital records 	<ul style="list-style-type: none"> • Risk scoring of transactions using similar analytics and common use cases based on timing, destination, source, value and frequency, device, and geolocation intelligence 	<ul style="list-style-type: none"> • Common feedback loop to develop a holistic view on modus operandi and drive top-down use-case development • Pooling of resources and capabilities

1. **Collaborative model.** In this model, which for most banks represents the status quo, each of the domains—financial crime, fraud, and cybersecurity—maintain their independent roles, responsibilities, and reporting. Each unit builds its own independent framework, cooperating on risk taxonomy and data and analytics for transaction monitoring, fraud, and breaches. The approach is familiar to regulators, but offers banks little of the transparency needed to develop a holistic view of financial-crime risk. In addition, the collaborative model often leads to coverage gaps or overlaps among the separate groups and fails to achieve the benefits of scale that come with greater functional integration. The model’s reliance on smaller, discrete units also means banks will be less able to attract top leadership talent.
2. **Partially integrated model for cybersecurity and fraud.** Many institutions are now working toward this model, in which cybersecurity and fraud are partially integrated as the second line

of defense. Each unit maintains independence in this model but works from a consistent framework and taxonomy, following mutually accepted rules and responsibilities. Thus a consistent architecture for prevention (such as for customer authentication) is adopted, risk-identification and assessment processes (including taxonomies) are shared, and similar interdiction processes are deployed. Deeper integral advantages prevail, including consistency in threat monitoring and detection and lower risk of gaps and overlap. The approach remains, however, consistent with the existing organizational structure and little disrupts current operations. Consequently, transparency is not increased, since separate reporting is maintained. No benefits of scale accrue, and with smaller operational units still in place, the model is less attractive to top talent.

3. **Unified model.** In this fully integrated approach, the financial crimes, fraud, and cybersecurity operations are consolidated into a single

The three models address financial crime with progressively greater levels of operational integration.

	Traditional: collaboration	Ongoing: partial integration¹	Future: complete integration
Model features	<ul style="list-style-type: none"> • Independent reporting, roles, and responsibilities for each type of financial crime • Independent framework built by each unit 	<ul style="list-style-type: none"> • Each financial-crime unit maintains independence but uses a consistent framework and taxonomy with agreed-upon rules and responsibilities: <ul style="list-style-type: none"> – Fraud and cybersecurity join on prevention (eg, on customer authentication) – Consistent processes for risk identification and assessment – Similar processes (eg, interdiction) 	<ul style="list-style-type: none"> • Consolidated unit under a single framework using common assets and systems to manage risks: <ul style="list-style-type: none"> – Single view of the customer – Shared analytics
Pluses and minuses	<ul style="list-style-type: none"> + Least disruptive: maintains the status quo + Regulators most familiar with the model - Less visibility into overall financial-crime risk - Potential gaps, overlap among groups - No scale benefits - Smaller units less able to attract top talent 	<ul style="list-style-type: none"> + More unified approach with lower risk of gaps/overlaps + Consistent organizational structure with status quo + Limited disruption from current state - Maintains separate reporting; does not increase transparency - No scale benefits - Smaller units less able to attract top talent 	<ul style="list-style-type: none"> + Underlying risks are converging + Enhanced ability to attract and retain talent + Standard and common framework on what is being done + Benefits of scale across key roles - Largest organizational change - While converging, risks remain differentiated - Regulators are less familiar with setup



Banks have begun by closely integrating cybersecurity and fraud while stopping short of a fully integrated unit

¹Mainly cybersecurity and fraud.

framework, with common assets and systems used to manage risk across the enterprise. The model has a single view of the customer and shares analytics. Through risk convergence, enterprise-wide transparency on threats is enhanced, better revealing the most important underlying risks. The unified model also captures benefits of scale across key roles and thereby enhances the bank’s ability to attract and retain top talent. The disadvantages of this model are that it entails significant organizational change, making bank operations

less familiar to regulators. And even with the organizational change and risk convergence, risks remain differentiated.

The imperative of integration

The integration of fraud and cybersecurity operations is an imperative step now, since the crimes themselves are already deeply interrelated. The enhanced data and analytics capabilities that integration enables are now essential tools for the prevention, detection, and mitigation of threats.

Most forward-thinking institutions are working toward such integration, creating in stages a more unified model across the domains, based on common processes, tools, and analytics. AML activities can also be integrated, but at a slower pace, with focus on specific overlapping areas first.

The starting point for most banks has been the collaborative model, with cooperation across silos. Some banks are now shifting from this model to one that integrates cybersecurity and fraud. In the next horizon, a completely integrated model enables comprehensive treatment of cybersecurity and financial crime, including AML. By degrees, however, increased integration can improve the quality of risk management, as it enhances

core effectiveness and efficiency in all channels, markets, and lines of business.

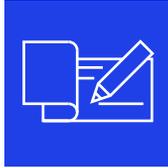
Strategic prevention: Threats, prediction, and controls

The idea behind strategic prevention is to predict risk rather than just react to it. To predict where threats will appear, banks need to redesign customer and internal operations and processes based on a continuous assessment of actual cases of fraud, financial crime, and cyberthreats. A view of these is developed according to the customer journey. Controls are designed holistically, around processes rather than points. The approach can significantly improve protection of the bank and its customers (Exhibit 6).

Exhibit 6

With a ‘customer journey’ view of fraud, banks can design controls with the greatest impact.

Potential fraud attacks in a customer journey, retail-banking example

	 Open an account	 Change account	 Make a payment	 Make a deposit
Customer-initiated actions	Customer opens a new account or adds another account through online, mobile, branch, or ATM channels	Customer updates existing account, eg, adding a beneficiary or changing address	Customer pays self or third party through wire, credit or debit card, or online transaction	Customer makes a transfer or deposit into their account
Attack channel				
ATM	<ul style="list-style-type: none"> • Identity theft • Synthetic ID • Employee-generated account • Malware 	<ul style="list-style-type: none"> • Malware 	<ul style="list-style-type: none"> • Card skimming or trapping • Fake PIN pad • Cash trapping • Shoulder surfing • Duplicate card • Malware • Transaction reversal 	<ul style="list-style-type: none"> • Money laundering or terror financing • Malware (balance multiplier)
Cards and e-commerce		<ul style="list-style-type: none"> • Account takeover • Address change • Secondary card • Malware 	<ul style="list-style-type: none"> • Card-not-present fraud • Card skimming • Malware • Cyberattack 	
E-banking and wire		<ul style="list-style-type: none"> • Addition of false beneficiary • Account takeover • Malware 	<ul style="list-style-type: none"> • Cyberattack • Malware • Employee-driven transaction 	
Branch		<ul style="list-style-type: none"> • Account takeover 	<ul style="list-style-type: none"> • n/a 	

To arrive at a realistic view of these transgressions, institutions need to think like the criminals. Crime takes advantage of a system's weak points. Current cybercrime and fraud defenses are focused on point controls or silos but are not based on an understanding of how criminals actually behave. For example, if banks improve defenses around technology, crime will migrate elsewhere—to call centers, branches, or customers. By adopting this mind-set, banks will be able to trace the migratory flow of crime, looking at particular transgressions or types of crime from inception to execution and exfiltration, mapping all the possibilities. By designing controls around this principle, banks are forced to bring together disciplines (such as authentication and voice-stress analysis), which improves both efficacy and effectiveness.

Efficiencies of scale and processes

The integrated fraud and cyber-risk functions can improve threat prediction and detection while eliminating duplication of effort and resources. Roles and responsibilities can be clarified so that no gaps are left between functions or within the second line of defense as a whole. Consistent methodologies and processes (including risk taxonomy and risk identification) can be directed toward building understanding and ownership of risks. Integrating operational processes and continuously updating risk scores allow institutions to dynamically update their view on the riskiness of clients and transactions .

Data, automation, and analytics

Through integration, the anti-fraud potential of the bank's data, automation, and analytics can be more fully realized. By integrating the data of separate functions, both from internal and external sources, banks can enhance customer identification and verification. Artificial intelligence and machine learning can also better enable predictive analytics when supported by aggregate sources of information. Insights can be produced rapidly—to establish, for example, correlations between credential attacks, the probability

of account takeovers, and criminal money movements. By overlaying such insights onto their rules-based solutions, banks can reduce the rates of false positives in detection algorithms. This lowers costs and helps investigators stay focused on actual incidents.

The aggregation of customer information that comes from the closer collaboration of the groups addressing financial crime, fraud, and cybersecurity will generally heighten the power of the institution's analytic and detection capabilities. For example, real-time risk scoring and transaction monitoring to detect transaction fraud can accordingly be deployed to greater effect. This is one of several improvements that will enhance regulatory preparedness by preventing potential regulatory breaches.

The customer experience and digital trust

The integrated approach to fraud risk can also result in an optimized customer experience. Obviously, meaningful improvements in customer satisfaction help shape customer behavior and enhance business outcomes. In the context of the risk operating model, objectives here include the segmentation of fraud and security controls according to customer experience and needs as well as the use of automation and digitization to enhance the customer journey. Survey after survey has affirmed that banks are held in high regard by their customers for performing well on fraud.

Unified risk management for fraud, financial crime, and cyberthreats thus fosters digital trust, a concept that is taking shape as a customer differentiator for banks. Security is clearly at the heart of this concept and is its most important ingredient. However, such factors as convenience, transparency, and control are also important components of digital trust. The weight customers assign to these attributes varies by segment, but very often such advantages as hassle-free authentication or the quick resolution of disputes are indispensable builders of digital trust.

The target fraud-risk operating model: Key questions for banks

In designing their target risk operating model for financial crimes, fraud, and cybersecurity, leading banks are probing the following questions.

— *Processes and activities*

- What are the key processes or activities to be conducted for customer identification and authentication, monitoring and detection of anomalies, and responding to risks or issues?
- How frequently should specific activities be conducted (such as reporting)?
- What activities can be consolidated into a “center of excellence”?

— *People and organization*

- Who are the relevant stakeholders in each line of defense?

- What skills and how many people are needed to support the activities?

- What shared activities should be housed together (for example, in centers of excellence)?

- What is the optimal reporting structure for each type of financial crime—directly to the chief risk officer? To the chief operations officer? To IT?

— *Data, tools, and technologies*

- What data should be shared across cybersecurity, fraud, and other financial-crime divisions? Can the data sit in the same data warehouses to ensure consistency and streamlining of data activities?
- What tools and frameworks should converge (for example, risk-severity matrix, risk-identification

rules, taxonomy)? How should they converge?

- What systems and applications do each of the divisions use? Can they be streamlined?

— *Governance*

- What are the governance bodies for each risk type? How do they overlap? For example, does the same committee oversee fraud and cybersecurity? Does committee membership overlap?
- What are the specific, separate responsibilities of the first and second lines of defense?
- What measurements are used to set the risk appetite by risk type? How are they communicated to the rest of the organization?

A holistic view

The objective of the transformed operating model is a holistic view of the evolving landscape of financial crime. This is the necessary standpoint of efficient and effective fraud-risk management, emphasizing the importance of independent oversight and challenge through duties clearly delineated in the three lines of defense. Ultimately, institutions will have to integrate business, operations, security, and risk teams for efficient intelligence sharing and collaborative responses to threats.

How to proceed?

When banks design their journeys toward a unified operating model for financial crime, fraud, and cybersecurity, they must probe questions about processes and activities, people and organization, data and technology, and governance (see sidebar “The target fraud-risk operating model: Key questions for banks”).

Most banks begin the journey by closely integrating their cybersecurity and fraud units. As they enhance

information sharing and coordination across silos, greater risk effectiveness and efficiency becomes possible. To achieve the target state they seek, banks are redefining organizational “lines and boxes” and, even more important, the roles, responsibilities, activities, and capabilities required across each line of defense.

Most have stopped short of fully unifying the risk functions relating to financial crimes, though a few have attained a deeper integration. A leading US bank set up a holistic “center of excellence” to enable end-to-end decision making across fraud and cybersecurity. From prevention to investigation and recovery, the bank can point to significant efficiency gains. A global universal bank has gone all the way, combining all operations related to financial crimes, including fraud and AML, into a single global

utility. The bank has attained a more holistic view of customer risk and reduced operating costs by approximately \$100 million.

As criminal transgressions in the financial-services sector become more sophisticated and break through traditional risk boundaries, banks are watching their various risk functions become more costly and less effective. Leaders are therefore rethinking their approaches to take advantage of the synergies available in integration. Ultimately, fraud, cybersecurity, and AML can be consolidated under a holistic approach based on the same data and processes. Most of the benefits are available in the near term, however, through the integration of fraud and cyber operations.

Salim Hasham is a partner in McKinsey’s New York office, where **Shoan Joshi** is a senior expert; **Daniel Mikkelsen** is a senior partner in the London office.

Designed by Global Editorial Services
Copyright © 2019 McKinsey & Company. All rights reserved.