Winning the face-off against fraud

How the most effective financial institutions are outthinking the bad guys

IBM Institute for Business Value

Executive Report

Banking

IBM Banking

To succeed in today's increasingly complex and volatile environment, businesses need to drive operational excellence and enable collaboration across enterprise functions, develop higher quality leadership and talent, manage amid constant change and unlock new possibilities grounded in data. For more information about IBM Banking solutions, visit ibm.com/banking.

Fraud has become pervasive

Fraud is a top-of-mind concern for financial institutions, particularly as electronic banking and payments opened a new and relatively porous channel, which organized crime has exploited in some rather complex and profitable schemes. But some leading institutions have found ways to effectively counter the threat through practical transformation plans supported by emerging technologies related to big data and analytics. This report examines their best practices for fighting fraud, as well as for transforming operations to do so.

Executive summary

Financial crime control is a chief priority for most financial institutions around the world, as they continuously evaluate the best ways to safeguard their systems, their data and, ultimately, their clients. Indeed, fraud and cyber security are on the formal management committee agendas at least quarterly for 80 percent of institutions, according to our recent financial fraud survey.

Our survey of 500 banking and financial markets executives whose responsibilities include fraud prevention was conducted as part of the IBM 2015 Fraud in Financial Institutions Study. Our efforts to identify current capabilities, successes, challenges and best practices in controlling financial crime also included interviews with senior fraud executives from financial institutions and related trade associations around the world. (For more information about the research, see the *Study approach and methodology* section.)

Underscoring the challenges today's institutions face in fighting financial crimes, only 56 percent of the executives we surveyed believe their organizations are in reasonable control of fraud threats. And a significant number believe their fraud operations organizations are in need of a substantial overhaul.

Many of the largest institutions, those with total assets greater than USD 300 billion, have transformed or are in the process of transforming their fraud operations. These organizations were successful in developing compelling, multi-factored business cases that emphasize not only the potential to stem direct fraud losses, but also to lower operating costs and – even more important – better engage customers. All of the largest institutions indicated that they were at least in control of the fraud situation, with 52 percent designating their capabilities as a competitive differentiator.

14%

of banking executives view their institutions' counter fraud capabilities as a competitive differentiator.

42%

of banking executives believe their fraud operations are in need of an overhaul.

49%

of banking executives either wait for the customer to complain about fraud or can't detect it.

It's a different story for the smaller institutions, however. A large majority of executives from firms with total assets of USD 100 billion or less identified their organizations' financial crimes situation as threatened, deteriorating or critical. More than three fourths of the smaller institutions have not undertaken any significant efforts to upgrade their counter financial crimes capabilities recently, while fraud charge-offs as a percentage of revenue were significantly higher for this group. The smaller firms had more trouble justifying a business case and had more difficulty with existing underlying technology in terms of both functional adequacy and their ability to use it effectively.

The good news is that much can be done right now to improve counter fraud and financial crimes performance. Emerging technologies related to analytics, big data and processing speed can help improve the ability to detect and interdict fraud before the money moves. They also can assist in discovering complex cross-channel fraud schemes, such as those organized by international criminal gangs.

Do losses of USD 70 million a year get your attention?

Direct fraud charge-offs alone account for more than seven basis points (b.p.) of revenue for at least 70 percent of the institutions surveyed. For a bank with USD 100 billion total assets earning an average 10 billion in revenue, that would represent USD 70 million in identified losses per year – and that is just for the direct losses.

If the total cost of fraud is expanded to include operations costs, such as for alert management, investigations, system administration and customer service, the overall cost to the bank could easily double. Considering the array of operating expenses, it's not surprising that the majority of financial institutions surveyed complained that fraud operations are too costly for the value received, while 42 percent cited the need for a significant overhaul, and only half indicated they are adequately protected.

Key definitions

- Financial institutions – Banks and financial markets companies. We did not include insurance companies, money services businesses or payment specialists.
- Financial crimes – Customer-based fraud, money laundering and cyber-based data or customer credential theft for the purposes of access to and theft of funds in customer accounts. Internal fraud and overall data theft are not included for purposes of this study.
- Fraud detection – The process of identifying fraudulent customer transactions.
- Fraud discovery – The process of identifying significant patterns of fraudulent behavior among a historical log of individual customer transactions.

"The bank originally thought it was making good returns on a particular product despite direct fraud charge-offs. But when the cost of fraud was more broadly measured to include fraud operations, it was shown the product was actually losing money overall."

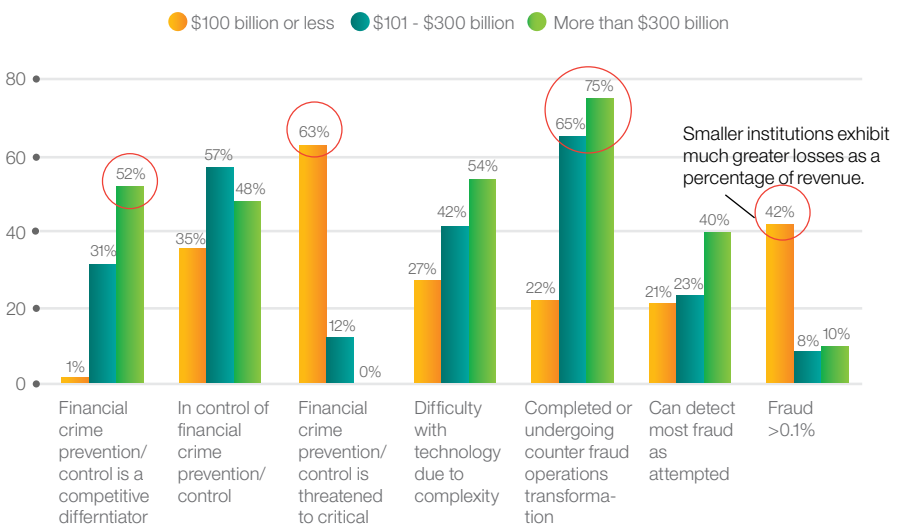
Chief security officer for a Canadian bank

Size matters

We found a correlation between institution size and overall fraud performance. All 48 of the executive respondents representing the largest institutions (those with total assets greater than USD 300 billion) indicated they are in control of their fraud situation, with 52 percent citing fraud control as a competitive differentiator. On the other end of the spectrum, 63 percent of the 315 smaller institutions (those with USD 100 billion or less in total assets) reported their situations as threatened, deteriorating or critical. And close to half (42 percent) of smaller institutions reported having direct fraud charge-offs greater than ten b.p. revenue (see Figure 1.)

Figure 1

Size matters: The smaller institutions feel more threatened; the larger ones are well on their way through transformation



Source: IBM 2015 Fraud in Financial Institutions Survey.
Note: Some percentages do not equal 100 due to rounding.

The disparity in performance is likely due to the larger institutions' initiative and budgetary capacity to undergo sizeable transformation programs that take advantage of technology advances in big data and analytics, processing speed and information access. Indeed, 75 percent of the largest institutions reported they were undergoing or had completed transformation programs, compared to just 22 percent of the smaller institutions. The middle-sized group – those with total assets between USD 101 and 300 billion – are in between, as expected. However, institutions in this middle group appear to be holding their own: 88 percent reported being in control or better of their fraud situation, and 65 percent reported they were in the process of conducting or had completed fraud operations transformation exercises.

Interestingly, while the smaller players indicated they were more threatened by fraud, 54 percent of the largest respondents reported difficulties with technical complexity and the ability to pull information together across the enterprise to detect the more complex fraud campaigns. The head of fraud technology for a U.K.-based top-tier global bank provided insight, saying, "It's not that we're too big to manage; it's that we're too complex."

"We recognize it's not an issue of adding more people to the fraud operation. Rather, it's a matter of working smarter with what we have – training, knowledge transfer, good sourcing."

Group head of financial crime and security for an ASEAN bank

Distinguishing leaders from the vulnerable

Survey data revealed that those institutions most effective in fighting financial crime tend to be large in size, have the ability to detect fraud in near real time, and be undergoing or have completed a major transformation in fraud operations.

Using cluster analysis based on factors including degree of fraud control, rate of fraud charge-offs, commitment to operational transformation and support of C-Suite, we identified three distinct groups and termed them: Differentiated Leaders, Capable Transformers and Exposed Neophytes. Differentiated Leaders primarily include both the largest industry players and our mid-sized USD 101 - 300 billion respondents. Differentiated Leaders reported relatively high degrees of fraud control, low rates of fraud charge-offs, strong commitment to operational transformation and C-Suite support for fraud strategy efforts.

The Exposed Neophytes group is primarily composed of the smaller institutions (94 percent have total assets between USD 10 and 100 billion). Most (84 percent) in this group reported fraud performance somewhere between threatened and critical. In addition, only 4 percent believe their technology is adequate and used effectively, compared to 48 percent of the Differentiated Leaders.

Between the two extreme clusters, but still well separated, are the Capable Transformers. Most in this group (79 percent) are from the USD 30 to 300 billion asset range and are behind in overall fraud capabilities (only 8 percent reported near real-time detection, while 73 percent reported write offs greater than seven b.p. revenue). However, Capable Transformers are either planning, in the middle of or at the conclusion of a transformation of their fraud operations. Another distinction of this group is that 65 percent agreed that their transformation programs are appropriately funded to meet institutional, customer and regulatory expectations.

What's working?

Operations

Gone are the days when sufficient fraud detection involved reliance on customers ringing the call center to dispute a charge on their credit card bills. Back then, fraud was fairly simple, opportunistic and individualized, such as when a lost credit card was picked up in the mall parking lot and used for a shopping spree. As the global head of fraud operations for a U.S. bank explained during our interview, although it could take two months to block the card from time of initial incident, the loss ratios were fairly small and generally acceptable as a "cost of doing business."

Now, it's estimated that 80 percent of consumer fraud is perpetrated by organized criminal gangs using multiple product channels, multiple locations, an easily recruited cadre of labor and a very short – sometimes only hours-long – campaign window for execution.[1] In 2013, for example, USD 45 million was stolen from automated teller machines in 27 countries in two attacks on separate days that collectively took only ten hours. The campaign involved hacking into credit and debit card payment processing networks, increasing account balances to allow large excess withdrawals, and distributing the stolen debit card information to over 100 accomplices worldwide who then conducted fraudulent withdrawals.[2]

The good news is that while organized crime has migrated into this easily executed and sometimes difficult to prosecute financial fraud environment, the technology to prevent and fight financial crime has improved by an order of magnitude. Groundbreaking advances in big data and analytics solutions, as well as processing speed, are differentiating the Leaders from those more reticent to transform. Technology solutions are helping Differentiated Leaders excel in several key areas:

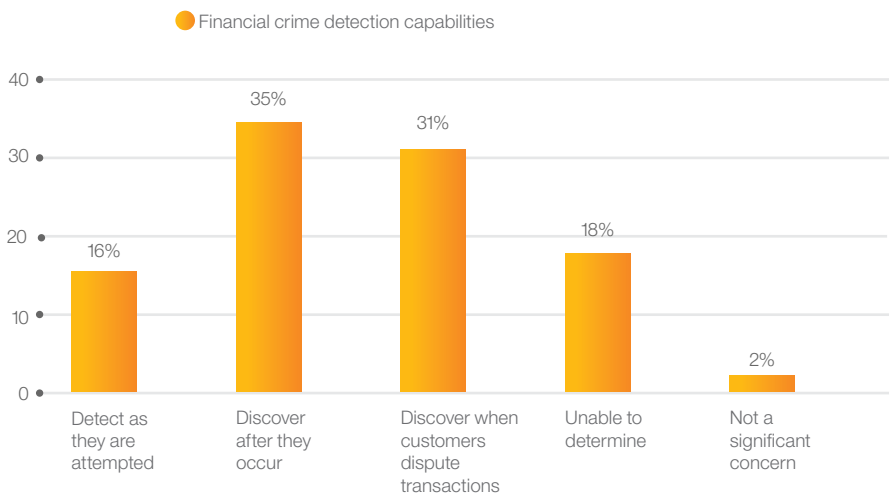
"Prosecuting fraud is not a priority for law enforcement, so it's better for us to interdict than it is to pursue investigations and recoveries. Law enforcement usually only catches the mules, not the real operators."

Head of global fraud management for U.S.-based money center bank

- *Real-time detection* (the ability to interdict a fraudulent transaction before it is settled) – If a transaction can be identified as fraudulent and stopped before funds are moved, the processing institution avoids investigative and recovery costs, the customer is not inconvenienced, and no money is lost. Only 16 percent of the institutions in our survey cited the ability to detect fraud as it was attempted, a key factor in differentiating their effectiveness in fighting fraud (see Figure 2). Regrettably, 31 percent still rely on customers disputing transactions, and another 18 percent are unable to determine how fraud was perpetrated.

Figure 2

Most financial institutions detect fraud after the fact



Source: IBM 2015 Fraud in Financial Institutions Survey.

- *Fraud and analytics expertise* – The most successful institutions employ individuals who have both deep analytical skills and seasoned expertise in counter fraud. While 69 percent of our respondents use analytics to discover fraud patterns, data and statistical scientists are typically housed in a different department or location than employees engaged in fraud operations. As a result, there is still a disconnect between the two groups that hampers the analytic process. Differentiated Leaders have realized the combination of data science and fraud prevention skills can facilitate detection of changing fraud patterns and the ability to make timely adjustments to stop losses. Since finding or training multi-skilled analysts can be rather difficult, many astute organizations have begun to combine or at least co-locate the two groups to intensify their interaction and, consequently, cross training.
- *Centralized operations* – Taking the co-location idea a bit further, many leading institutions are beginning to combine their enterprise-wide fraud and analytics expertise into "centers of excellence." Centralization not only leverages the effectiveness of the combined skill sets, but also helps standardize and simplify methods and technology, which can help lower operating costs. In discussing his organization's strategy, the head of global fraud technology for a U.K.-based bank commented, *"*We're building a big ecocentric network with a center of excellence for fraud analysis and a centralized data base where we dump all the alerts and other information. We'll use it as kind of a sandbox to conduct our analyses. It helps us offset the problem of bifurcated detection systems across the enterprise.*"*

"We combined the analytics and fraud operations staff together and co-located them, which provided the facility to share ideas and expertise and improve overall counter fraud effectiveness."

Head of group security and business resilience for an Australian bank

- *Broader information sets* – Both the amount and availability of data have mushroomed over the past decade, and the technology to manage and leverage information continues to evolve as well. In fraud prevention efforts, the inclusion of additional relevant information in the analysis can translate into improved detection rates, lower false positives and lower operating costs for alert management and investigations. However, while most institutions use internal transaction and customer data to analyze criminal behavior, less than half are using additional information from external sources, and only 34 percent are sharing crime intelligence with their competitors. Many are having difficulty managing their own information. Reflecting this, the most cited and desired capability for improving financial crime controls was the ability to link criminal activity across divisions and product channels. Indeed, as well-organized fraudsters often attack several product channels and separate institutions in a single campaign, big data and cross-competitor collaboration become essential.
- *Customer engagement and satisfaction* – Leading institutions have discovered that informing and engaging with customers about fraud control can help positively impact program effectiveness and customer satisfaction. Fourteen percent of survey participants indicated that their organizations' effectiveness in controlling and preventing financial crimes is a competitive differentiator, and customer impact was cited as the leading factor in justifying and approving investments in fighting financial crimes. Those institutions with the most effective programs are able to mitigate the tradeoff between control and customer convenience through better, non-intrusive technologies.

Technology

We mentioned above that the emergence of advanced big data and analytics technologies combined with huge increases in processing speed can help provide the means to counter the multi-channel, rapidly executed fraud campaigns of organized criminal gangs. Our research has revealed some best practices in utilizing these technologies:

- *Multifaceted solutions* – Through our interviews, we discovered that many organizations successful in controlling financial crime apply a number of different controls even if they overlap. The most successful institutions are implementing tools and processes for cyber security, entity resolution (relationship analytics), malware detection, pattern analysis and real-time transaction scoring in combination. But there are limits as to how much can be practically deployed. Said one chief security officer of a top Canadian bank, who also had enterprise-wide fraud responsibility, "We can't do it all; it's impossible to anticipate, identify and protect against everything. Instead we need to focus our protection on the nexuses and places where we can practically implement the protective and detective measures."
- *Analytic agility* – The cycle time between discovery of a new fraud pattern and the subsequent adjustments to the transaction scoring process to interdict it is a key factor. Of the Exposed Neophytes, 91 percent reported a cycle time of four weeks or greater just to discover the pattern, and 84 percent reported requiring at least another four weeks to update their scoring engines – for a total cycle time of eight weeks or greater. Within that eight-week cycle, fraud within that pattern will persist. At the other end of the spectrum, 24 percent of the Differentiated Leaders reported their organizations took less than four weeks to discover fraud, and 34 percent indicated less than four weeks to update their transaction scoring process.

"We can't do it all; it's impossible to anticipate, identify and protect against everything. Instead we need to focus our protection on the nexuses and places where we can practically implement the protective and detective measures."

Chief security officer for a Canadian bank

We also discovered that effectively using new technology involves a learning curve for many organizations. While 22 percent of all respondents indicated their technology was adequate and used effectively, the remainder reported that their technology was too complex (22 percent), not used effectively (39 percent) or inadequate overall (17 percent). Clearly, training and platform simplification are important. A group head of fraud and security for a top ASEAN bank explained the issues facing his team, declaring, "We've made millions of dollars in investments in technology, primarily what we perceived to be best-of-breed, depending on the immediate need. As a result, we have a huge integration problem and can't make sense of the information we have."

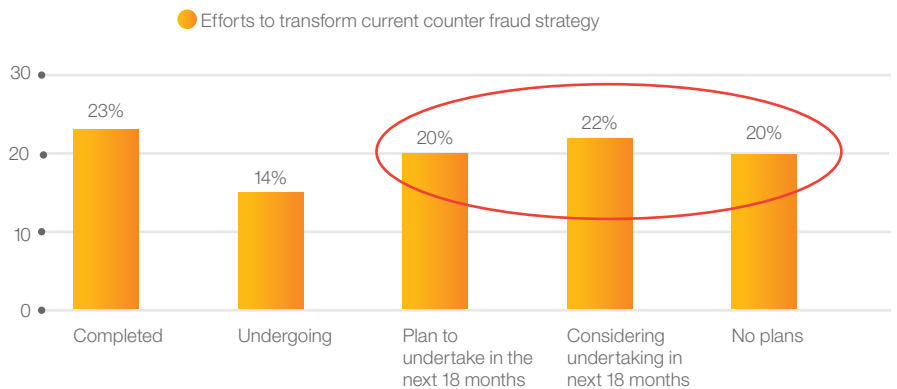
Making transformation happen

Most institutions have not undergone a fraud transformation program, and 20 percent have no plans to do so (see Figure 3). The two most salient obstacles cited by respondents are perceived cost versus benefit and the availability of skilled staff or outside consultants.

When looking at clusters, however, we found that the majority of Differentiated Leaders have either completed (39 percent) or are undergoing (22 percent) transformation initiatives related to fraud operations and technology. The Exposed Neophytes, on the other hand, are woefully behind (only 9 percent completed and another 9 percent undergoing) or have no plans for transformation at all (37 percent).

Figure 3

Most institutions haven't started a fraud transformation program



Source: IBM 2015 Fraud in Financial Institutions Survey.

Another natural aversion to transformation initiatives is that they tend to be rather large, those for fraud being no exception. Most (85 percent) of the transformation programs either underway or completed by our survey participants required at least six months, and over a quarter (28 percent) involved more than 18 months. Similarly, of the initiatives either completed or underway, 64 percent were cited as costing more than USD 2 million.

Transformation initiatives require strong business cases to compete for always limited funds. While the resultant savings in direct fraud charge-offs can be substantial, they are often insufficient to raise the initiative above the cut-off line for the institution's strategic initiatives. Most of the institutions from our survey that are undergoing or have completed fraud

The most popular justifications for fraud transformation initiatives were customer impact and potential reduction in operating costs.

transformations used several factors (68 percent used three or more) in their business cases, with the impact on the customer the most popular (used by 47 percent). The head of financial crimes technology for a top Australian bank explained, "The bank's culture is all about customer service. We found that when we describe fraud improvement as an impact on the customer experience, we get a lot more executive support."

The second most widely used factor in successful transformation business cases is the potential reduction in operating costs. For example, one of the most significant impacts of better analytics in the fraud space is the improvement in the effectiveness of fraud transaction scoring. As experienced by a U.S.-based top-tier global bank that we interviewed, a well implemented analytic solution can yield a 100 percent improvement in fraud detection rates (true positives), with a 30 percent reduction in false alerts (false positives). The resultant alert load lightening on the fraud investigations staff, usually a huge department, can sometimes yield operating cost savings greater than the charge-offs themselves.

Other factors that were used to justify investments in fighting financial crimes cited by more than 20 percent of the 500 respondents include operational stability (36 percent), impact on transaction processing (22 percent), customer retention (33 percent) and even revenue enhancement (29 percent).

Finally, as with all significant investments, support from the C-Suite, particularly the CEO, is critical to get the program off the ground. We received an interesting comment from the head of fraud operations at a U.S.-based top-tier institution, who said, "Seems like the banks that have the most fraud engagement and support from the CEO are those that have been recently burned." Is it only a matter of time?

Execution – How to successfully transform

Let's assume the business case is justified, the CEO is on board, and the rest of the C-Suite is convinced that an improvement in counter fraud performance would provide quite a lift to the customer satisfaction surveys. What can be learned from those who have traveled this road before and tackled financial crimes by transforming their fraud operations? What are some of the best transformation strategies and what strategies should be avoided?

First, it's important to realize that transformation programs are not "plug and play." As described above, most require at least six months elapsed time (often longer). And, as our survey also revealed, they are not cheap. A realistic plan in terms of time and cost is crucial. Of the 117 institutions from the survey that have actually completed transformations, 47 percent adopted an incremental approach. Our interviews revealed several ways to approach an incremental roll out:

- Many institutions replace obsolete legacy systems sequentially, usually starting with the most ineffective systems.
- A number of organizations apply a rather simple set of detection rules at the outset and use subsequent rule testing and other analytics to improve the models and rules over time.
- Some institutions apply the transformation on a business unit by business unit basis, usually with the same or similar technology platforms to avoid the cost and complexity of duplicated systems.

Second, intelligent choices about what improvements and capabilities are really necessary can help drive both the cost versus benefit business case and help simplify operations. The head of a Singapore-based mid-sized bank explained the importance of choices and an overall strategy, saying, "We've made a lot of investment in fraud and security systems over the past five to seven years, but it has not been all that coordinated. Rather, we bought the perceived best-of-breed, depending on tactical or specific channel needs, without regard to enterprise-wide standards or strategy, which weren't in existence at the time."

Learning from the Differentiated Leaders

While there is a fairly wide disparity in the maturity of financial institutions' capabilities in fighting fraud, there is much to learn from the Differentiated Leaders, including use of the following:

- *Real-time detection* – so that fraud is interdicted before losses and recovery expenses are incurred
- *Agile analytics* – to quickly detect the constantly morphing patterns in criminal behavior
- *Broader information sets* – to expand understanding and make better decisions about each customer transaction
- *Multifaceted defenses* – that anticipate complex criminal behavior along several channels, leaving no single point of potential failure.

Ready or not? Ask yourself these questions

- How would you describe your company's ability to fight financial crimes?
- What factors might be contributing to inefficiencies in your fraud investigations unit (staff and infrastructure)?
- What methods do you employ to ensure that your institution can identify and prevent newly emerging fraud patterns?
- What capabilities do you have to actually interdict fraud before a transaction is settled or money is moved?
- How are you using analytics to determine emerging fraud patterns at your institution?
- How do your customers view your institution's ability to protect them from fraud?

For more information

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our monthly newsletter, visit: ibm.com/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for your phone or tablet from your app store.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Global Business Services, develops fact-based strategic insights for senior business executives around critical public and private sector issues.

About the authors

Wilson Davis is an Associate Partner, Strategy and Analytics, Fraud, for IBM Global Business Services. Wilson specializes in financial and operational data analytics, counter fraud and anti-money laundering, straight-through-processing, IT department transformations and game-changing improvements in business processes and application systems for the financial services industry. He holds an MBA from the Tuck School of Business at Dartmouth and has ten years' experience as a Fortune 500 IT executive and 15 as a partner-level consultant. He can be reached at ewdavis@us.ibm.com.

David Dixon is the Worldwide Financial Crime Industry Leader, IBM Analytics. An established expert in global anti-fraud, anti-money laundering and anti-terrorism programs for financial institutions, David is a frequent speaker at international conferences. Previously, he led the development and delivery of industry-leading financial crime solutions for Norkom Technologies, as well as Bearing Point practice. David spent ten years at the Bank of Montreal, with responsibility for electronic monitoring of fraud, AML and anti-terrorist financing. He can be reached at ddixon@ca.ibm.com.

Contributors

Hester Ngo, IBM Canada, Analytics; Rick Hoehne, IBM Global Business Services; Eric Lesser, IBM Institute for Business Value; Maribeth Mallon Haynes, IBM Analytics; Scott Burroughs, IBM Analytics; David Dixon, IBM Canada, Analytics; Austin Wells, IBM Analytics; Samiran Mukhopadhyay, IBM Sales and Distribution; and Angus Stewart, IBM Australia, Software Sales.

Study approach and methodology

During the month of September 2015, IBM engaged Oxford Economics to conduct an independent electronic survey of global banks and financial markets companies about their capabilities in fighting financial crimes. The 500 responses from executives charged with fraud prevention operations represented a broad sample across geographic region and asset size.

In addition to conducting the survey, we interviewed senior fraud executives in financial institutions broadly reputed as leaders in financial crime control and executives from related trade associations. We asked questions about their successes, challenges and best practices related to fighting financial crimes and successfully transforming their organizations to do so. Through their fascinating insights, we discovered some interesting diversity in successful methods.

As financial crime information and operating practices are highly sensitive and regularly kept confidential, both the electronic survey and the direct interviews were conducted with the promise that names of the institutions and individual respondents would remain anonymous. The individual quotes and statistics are real, though in some cases, executive titles were changed to protect from direct attribution.

Notes and sources

1. "Comprehensive Study on Cybercrime." United Nations Office on Drugs and Crime. February 2013. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

2. Vaughan, Bernard. "Six arrested in $45 million global cybercrime scheme." Reuters. November 18, 2013 (accessed November 16, 2015). http://www.reuters.com/article/2013/11/18/us-usa-crime-cybercrime-idUSBRE9AH0YZ20131118#o5jDlKhY2i2bEeVO.97

IBM Global Business Services
Route 100
Somers, NY 10589

Produced in the United States of America
January 2016

GBE03726-USEN-01