Making a business case for fraud-prevention technology

Evaluate the true impact of fraud on financial institutions—and the full implications of fraud-prevention solutions

Contents

Introduction

Building a business case to justify fraud-prevention technology investments is, unfortunately, not as straightforward as one might expect. The impact of online fraud on a financial institution is multifaceted and complex. Fraud incidents and fraud-prevention efforts affect many aspects of the bank's services and customer interactions. A realistic, robust business case should consider a broad array of components, beyond fraud loss reduction and fraud management operating costs.

Based on extensive discussions with client financial institutions, IBM has defined and categorized the key business case components that should be taken into consideration when examining the business ramifications of various technology approaches. Each bank will weigh the factors differently, so what one bank may consider critical another bank may consider ancillary. However, with tightened budgets and the challenges typically faced by cost centers, it behooves all financial institutions to recognize the true impact of fraud on their organization, as well as the full implications of available fraud-prevention technologies. Those that understand the devastating capabilities of advanced malware also understand that the industry cannot afford to skimp on malware-prevention technology.

IBM has collected and categorized the components that have been the primary drivers for our customers' fraud technology business cases. This white paper explains how each component can help financial institutions create a realistic return on investment (ROI) model. Where available, metrics are provided for the components. Otherwise, we provide a list of considerations that IBM clients have used in their business cases.

Fraud loss avoidance

A primary goal of fraud-prevention technology is preventing fraud losses—that is, unrecovered stolen funds. Financial institutions should consider the impact of fraud-prevention technology on reducing fraud across the following categories.

Online-channel fraud losses

Historical online-channel fraud losses should be readily available to financial institutions. Many financial institutions are actually more concerned with the potential for future losses considering the growing sophistication of malware and frequency of cybercrime attempts. For example, to bypass online risk engines, some malware is designed to adapt to user navigation and transaction behaviors to avoid exposing anomalies compared with the user's base profile.

Several top- and mid-tier financial institutions have reported an increase in fraud attempts as a result of fraud migrating from the "mega-banks." Because the largest financial institutions have implemented extensive, sophisticated fraud-prevention programs, cybercriminals are now turning their attention to the more vulnerable institutions that don't yet have the proper protection in place. One single incident could result in hundreds of thousands (if not millions) of dollars in fraud losses.

Cross-channel fraud losses

Criminals are increasingly stealing credentials online to commit fraud in other channels and avoid detection by online risk engines. Unfortunately, the vast majority of banks have no simple way of detecting this type of fraud, and therefore cannot determine the magnitude of cross-channel fraud to their institution. We expect cross-channel fraud to increase as cybercriminals generally take the path of least resistance.

An example of cross-channel fraud that was recently uncovered by IBM, took the form of an elaborate check-fraud scheme. Criminals used malware to access bank accounts and view check images, collect transaction histories, and access other business data. This information was used to create sophisticated counterfeit checks, backed by detailed knowledge of account and transaction histories. In this example, the bank would ultimately classify this fraud as check fraud without realizing that the information required to commit the fraud was initially gained online. One IBM client reported a 30 percent reduction in check fraud for customers protected by IBM® Security Trusteer Rapport, as compared to customers using other solutions or no protection at all. Because criminals could not access accounts protected by Trusteer Rapport, they could not commit this type of cross-channel check fraud.

Another IBM client experienced a 93 percent reduction in contact-center fraud cases after implementing IBM solutions. The client attributed the reduction to blocking fraudulent access to online accounts so that criminals could not gather the information necessary to impersonate legitimate customers at the contact center. Other clients have shared the impact of IBM Security Trusteer endpoint-protection products on reducing wire and debit card fraud, among others.

Component	Sample metrics
Online-channel fraud losses	One bank is likely liable for USD345,000 fraud loss in the Patco suit
	Another bank is likely liable for USD560,000 fraud loss in the Experi-Metal suit
	Most banks express the sentiment, "It only takes one major incident to cause significant damage"
Cross-channel fraud losses	One client reported a 30 percent reduction in check fraud for customers protected by Trusteer Rapport
	One client reported a 93 percent reduction in contact-center fraud cases after implementing IBM® Security Trusteer Pinpoint Criminal Detection
	IBM estimates that most banks can expect to reduce fraud in other channels by 20 to 30 percent using IBM Security Trusteer solutions

Fraud-management costs

Financial institutions require significant resources to manage and monitor online sessions and transactions to identify potential fraud. Even the best risk-based fraud detection systems generate a tremendous number of false positive alerts—that is, potentially fraudulent transactions that are actually legitimate transactions. Fraud analysts may investigate dozens of alerts in order to identify one that represents an actual fraudulent transaction.

Fraud-prevention costs

Financial institutions have myriad options for building and maintaining their fraud-prevention infrastructure. A number of authentication and fraud-detection technologies are often deployed (with various levels of integration) that generally require significant employee resources for ongoing operations and maintenance. Fraud engines often require a substantial upfront investment to create and integrate the data feeds required for analysis. These systems then demand significant resources on an ongoing basis to investigate false positives, such as hiring fraud analysts for alert investigation and customer outreach, contact-center agents to answer calls when transactions are blocked or re-authenticated, and payment operations staff to reverse or recover identified fraudulent payments.

The more effective any single technology is at preventing fraud, the fewer technologies are required to fill in the gaps. Technologies that prevent fraudulent transactions before they are even initiated are preferable to those that attempt to find fraudulent transactions along the payment processing flow. Both are necessary as part of a strong layered security platform, but the former is far more cost effective and reliable as a fraud-prevention tool.

Several IBM clients have reported a 50- to 99-percent reduction in false positive alerts generated by their risk engines. Trusteer Rapport blocks virtually all malware-based fraud attempts so that no fraudulent transactions enter the payment processing system.

IBM® Security Trusteer Pinpoint Malware Detection accurately detects the presence and severity of malware on end user devices, greatly improving the accuracy of risk-engine analytics.

Fraud-remediation costs

When fraud transactions occur successfully, additional internal and external resources are often required to communicate with the customer and then investigate and potentially prosecute the event. Larger publicly disclosed events also require public relations and legal intervention. Commercial clients are increasingly turning to lawsuits to recover funds stolen through cyber-fraud events. Many of these cases are settled out of court, but not without significant legal costs and internal resource demands.

Virtually eliminating fraud virtually eliminates fraud-remediation costs. IBM clients can avoid these expenses because fraudulent transactions are not allowed to enter the processing system where they can be missed by authentication and fraud-risk engines.

Malware-remediation impact

When a customer device is suspected of containing malware, the financial institution must ensure that the malware is removed in order to help avoid fraud. Many financial institutions require their customers to self-remediate, which often involves their using a third-party service. This expense is often borne by the customer (with significant inconvenience) and sometimes by the bank. In either case, the bank utilizes specialized customer service representatives or third-party resources to resolve the problem with the customer. If the customer self-remediates, the bank has no guarantee that the malware was actually removed—or that the customer even tried to remove the malware.

Trusteer Rapport can be used to remove malware—either by completely erasing or destroying it—from a customer's device. No customer action is required and the bank has full visibility into the condition of the customer's device to help ensure malware removal is accomplished. More importantly, this service positions the bank as a customer advocate and, in turn, customers are extremely appreciative when their bank provides what would otherwise be a challenging task.

Component	Sample metrics
Fraud-prevention costs	IBM clients report reducing false-positive alerts by 50 to 90 percent
	Several large clients displaced fraud analysts due to a marked reduction in false positive alerts using IBM Security Trusteer solutions
	Several clients shared that eliminating malware-based fraud helped eliminate the need for additional technology solutions
Fraud-remediation costs	Internal staff, executive or board-of-director involvement is time consuming and costly
	External legal, public relations and expert consulting is costly
Malware-remediation impact	Reduced bank expenses for internal specialists or third-party remediation
	Eliminated the issue of validating effective malware removal on customer devices

Compliance and legal costs

The highly regulated nature of the financial services industry places a tremendous burden on financial institutions to comply with a variety of requirements. The primary regulatory requirement driving financial institutions to upgrade fraud-prevention capabilities is the *Supplement to Authentication in an Internet Banking Environment*, issued by the Federal Financial Institutions Examination Council (FFIEC).[1] This FFIEC Guidance has been used to determine bank security expectations in recent lawsuits between banks and defrauded commercial banking customers. Financial institutions, therefore, must ensure their fraud-prevention platforms comply with the FFIEC Guidance, as well as other applicable regulations, and effectively prevent fraud to help avoid potential litigation.

FFIEC-related compliance risks

Many financial institutions have struggled with interpreting the FFIEC supplemental compliance requirements. While much of the industry has been slow in implementing FFIEC-compliant solutions, the time for compliance is now. The penalties for noncompliance may include fines, additional audits, sub-par examination ratings—which may affect insurance premiums—and reduced market confidence among investors, clients and employees.

The primary purpose of the FFIEC Guidance is to drive financial institutions to implement effective, sustainable fraud-prevention solutions. IBM Security Trusteer solutions address the key requirements for FFIEC compliance, including:

- **Risk assessment**—The FFIEC requires financial institutions to perform periodic risk assessments and adjust their customer authentication controls as appropriate in response to new threats to customers' online accounts. The IBM worldwide network of analysts continually monitors for new online threats and immediately updates defenses on every covered server and endpoint to mitigate the identified threat. For example, IBM Security Trusteer solutions defeat malware designed to steal out-of-band, one-time-password credentials. Otherwise, a financial institution would have to deploy new authentication technology to replace the compromised solution, leading to significant costs and customer disruption.
- **Layered security**—The FFIEC also requires financial institutions to implement a layered approach to security for high-risk Internet-based systems. While no single solution is ever sufficient to prevent fraud, IBM Security Trusteer solutions protect the weakest link in the online transaction chain, the customer's device. And IBM Security Trusteer solutions are designed with adaptable layers that specifically stop malware and phishing attempts on customer devices. Several IBM clients said that they were specifically looking for a solution that addressed the vulnerability of their customers' desktops, which is otherwise outside of the bank's control.

- **Threat landscape and compensating controls**—The FFIEC states that fraudsters are utilizing increasingly sophisticated and malicious techniques to thwart existing authentication controls, gain control of customer accounts and transfer funds to money mules that facilitate the movement of those funds beyond the reach of financial institutions and law enforcement. The agency focuses on malware-based attacks, including key-logger, man-in-the-browser and man-in-the-middle attacks. IBM provides effective solutions for specifically preventing these types of attacks. Several IBM clients are on record stating that their institutions have not suffered any losses due to malware-based attacks since deploying IBM Security Trusteer solutions.

Commercial account fraud litigation exposure

Recent court rulings, such as in the Patco and Experi-Metal cases, have dramatically changed the way the industry interprets the term "commercially reasonable security" described in UCC 4A. The traditional interpretation of "utilizing similar technologies as peer banks" is no longer sufficient. Banks must now also demonstrate that the appropriate fraud-prevention technologies are deployed and used appropriately.[2, 3]

The bottom line in addressing both regulatory compliance and litigation avoidance is simply this: prevent fraud. The FFIEC has focused on helping the industry prevent advanced online fraud threats and, more specifically, malware-based threats. The courts seem to be putting more responsibility on banks to actually protect their clients from fraud rather than simply going through the motions of implementing the same technologies as peer banks. Preventing fraud can help banks avoid the risks of noncompliance and litigation.

Component	Sample metrics
Regulatory compliance risk	Fines, sanctions and more due to noncompliance
	Overspending on unnecessary technologies due to assuming they are required or effective
	Several clients shared that eliminating malware-based fraud helped eliminate the need for additional technology solutions
Litigation exposure risk	Direct fraud losses absorbed by financial institutions
	Legal costs, both internal and external, including attorneys and expert witnesses
	Reputational damage with the public, investors, employees, regulators and customers
	Additional technology investments required to remediate the security flaws that allowed fraud

Customer impact

Financial institutions should implement fraud-prevention technologies that also have a positive impact on customer relationships. First and foremost, the solution should prevent fraud, but it is equally important that the solution is not burdensome to the customer. This burden can take the form of excessive or unnecessary contact during fraud investigations, demanding authentication procedures, or transaction and service limitations.

Brand impact

Following a fraud event, financial institutions should expect the affected customer to move some or all of his or her business to another institution. When fraud events become more public, banks also experience additional customer runoff due to diminished confidence. Some banks may not be able to withstand the disastrous ramifications associated with a major fraud event.

Many IBM clients state that their primary objective for preventing fraud is simply to "stay out of the paper." The cost for recruiting new business is far higher than nurturing and maintaining existing customers. With this substantial emphasis on customer retention, loyalty and confidence, many banks value brand protection above all else.

Customer convenience

Fraud-prevention procedures, when excessive, can weaken the quality of customer relationships. Requiring burdensome authentication procedures such as the use of hard tokens or excessive challenge questions can severely diminish the convenience offered by the online channel, causing it to be considered more of a nuisance. Even so-called "behind-the-scenes" anomaly-detection solutions can generate more false positive alerts—transactions identified as potentially fraudulent—than alerts about actual fraudulent transactions. This often results in customer contact to validate the transactions under investigation, which can lead to customer dissatisfaction when not handled properly.

In addition to providing effective fraud prevention, IBM Security Trusteer products require little to no customer intervention, unlike many authentication and fraud-prevention solutions. Beyond the fact that virtually all authentication approaches can be readily bypassed by advanced malware threats and social-engineering schemes, advanced authentication procedures can be time consuming or error prone for customers. And hardware-based technologies may not always be available when customers want to use online banking.

Furthermore, providing customers with automated fraud remediation can be a great tool for customer retention. Typical consumers and small businesses are challenged to recognize when their devices are infected with malware, let alone successfully remove the malware. While many free and pricey "malware-removal" tools are available, these are mostly glorified anti-virus applications that generally do a poor job of removing advanced malware threats, especially zero-day malware. When the bank steps in to identify and fix a customer's malware problem, it can create long-term goodwill and customer loyalty.

Positive customer benefits

Delineating the potential negative ramifications of "bad" fraud-prevention practices is somewhat obvious. What is sometimes less obvious is how "good" fraud-prevention practices can enhance customer relationships. Recent academic research demonstrates empirically tested positive associations between the activities banks undertake to protect customers from fraud and customer relationship quality and loyalty. The study found

that banks have experienced an increase in customer satisfaction, loyalty, trust and cross-buying intentions by providing meaningful fraud-prevention tools.[4] This influence is especially true for customers who have previously been victims of fraud.

As an example of the positive influence that customer-friendly fraud prevention can have, one IBM client reported a 33 percent increase in online banking adoption after proactively marketing Trusteer Rapport to its retail and commercial customer base. The bank believes that providing Trusteer Rapport demonstrates the bank's strong position on preventing fraud and protecting customers. This enhanced protection influenced those customers still concerned about online security to finally register for online banking.

Further, many banks now limit the breadth and depth of online service offerings due to the risk of online fraud. Many large banks do not provide online wire-transfer capabilities, and nearly all banks limit transaction amounts and frequencies to some extent. Better fraud-prevention capabilities can help reduce fraud risks, which will in turn allow banks to offer a wider variety of online capabilities with fewer transaction restrictions.

Component	Sample metrics
Brand impact	Third-party studies indicate that half of customers affected by fraud move their banking elsewhere
	Additional customer runoff can be expected after a publicly disclosed fraud event
	High customer-acquisition costs make customer retention a priority
Customer convenience	Burdensome authentication and excessive or unnecessary contact by fraud investigators reduces customer satisfaction
	Some advanced authentication procedures simply cannot be used by less technically savvy customers
	IBM Security Trusteer products are unobtrusive, yet noticeably present—the perfect blend for customer convenience and satisfaction
	Automated malware removal and potential expense avoidance can lead to enhanced customer service and customer satisfaction
	Proactive fraud protection can lead to enhanced customer satisfaction and loyalty
Positive customer benefits	Visible, yet unobtrusive fraud-prevention technologies demonstrate customer care and promote a positive brand image
	Better fraud-prevention capabilities enable financial institutions to provide broader sets of online services with fewer restrictions
	Proactively offering Trusteer Rapport led one bank to increase online banking adoption by 33 percent

Conclusion

It behooves every financial institution to find a fraud management solution set that effectively mitigates identified risks while being adaptable to future risk scenarios. Fraud techniques are continually evolving as fraudsters test for the weak spots in banks' armor, and are often quite inventive in finding vulnerabilities. Simply focusing on protecting the institution against known fraud will lead to a solution set that is obsolete the day it is implemented, due to the evolving nature of online fraud.

The business case for fraud-prevention technology should adequately represent the entire range of costs and benefits to the financial institution. Making this case enables fraud-prevention organizations to educate the appropriate lines of business required to gain broader support for technology investments. It can also demonstrate the value of implementing technologies that effectively prevent fraud while promoting a positive customer experience.

Business case component summary

Component	Sample metrics
Online-channel fraud losses	One bank is likely liable for USD345,000 fraud loss in the Patco suit
	Another bank is likely liable for USD560,000 fraud loss in the Experi-Metal suit
	Most banks express the sentiment, "It only takes one major incident to cause significant damage"
Cross-channel fraud losses	One client reported a 30 percent reduction in check fraud for customers protected by Trusteer Rapport
	One client reported a 93 percent reduction in contact-center fraud cases after implementing Trusteer Pinpoint Malware Detection
	IBM estimates that most banks can expect to reduce fraud in other channels by 20 to 30 percent using IBM Security Trusteer solutions
Fraud-prevention costs	IBM clients report reducing false-positive alerts by 50 to 90 percent
	Several large clients displaced fraud analysts due to a marked reduction in false positive alerts using IBM Security Trusteer solutions
	Several clients shared that eliminating malware-based fraud helped eliminate the need for additional technology solutions

Component	Sample metrics
Regulatory compliance risk	Fines, sanctions and more due to noncompliance
	Overspending on unnecessary technologies due to assuming they are required and effective
	Several clients shared that eliminating malware-based fraud helped eliminate the need for additional technology solutions
Litigation exposure risk	Direct fraud losses absorbed by financial institution
	Legal costs, both internal and external, including attorneys and expert witnesses
	Reputational damage with public, investors, employees, regulators and customers
	Additional technology investments required to remediate the security flaws that allowed fraud
Brand impact	Third-party studies indicate that half of customers affected by fraud move their banking elsewhere
	Additional customer runoff can be expected after a publicly disclosed fraud event
	High customer-acquisition costs make customer retention a priority
Customer convenience	Burdensome authentication and excessive or unnecessary contact by fraud investigators reduces customer satisfaction
	Some advanced authentication procedures simply cannot be used by less technically savvy customers
	IBM Security Trusteer products are unobtrusive, yet noticeably present—the ideal blend for customer convenience and satisfaction
	Automated malware removal and potential expense avoidance can lead to enhanced customer service and satisfaction
	Proactive fraud protection can lead to enhanced customer satisfaction and loyalty

Component	Sample metrics
Positive customer benefits	Visible, yet unobtrusive fraud-prevention technologies demonstrate customer care and promote a positive brand image
	Better fraud-prevention capabilities enable financial institutions to provide broader sets of online services with fewer restrictions
	Proactively offering Trusteer Rapport led one bank to increase online banking adoption by 33 percent

Why IBM?

IBM Security solutions are trusted by organizations worldwide for fraud prevention and identity and access management. The proven technologies enable organizations to protect their customers, employees and business-critical resources from the latest security threats. As new threats emerge, IBM can help organizations build on their core security infrastructure with a full portfolio of products, services and business partner solutions. IBM empowers organizations to reduce their security vulnerabilities and focus on the success of their strategic initiatives.

For more information

To learn more about IBM Security Trusteer solutions for fraud prevention, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM® X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
August 2014

Please Recycle

[1] Federal Financial Institutions Examination Council, "Supplement to Authentication in an Internet Banking Environment," June 28, 2011. http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20%28FFIEC%20Formated%29.pdf

[2] Linda McGlasson, "Inside the Comerica/Experi-Metal Case," BankInfo Security, http://www.bankinfosecurity.com/inside-comericaexperi-metal-case-a-2763/op-1, July 19, 2010.

[3] Tracy Kitten, "PATCO ACH Fraud Reversed," http://www.bankinfosecurity.com/patco-ach-fraud-rulingreversed-a-4919, BankInfo Security, July 4, 2012.

[4] Arvid O.I. Hoffmann and Cornelia Birnbrich, "The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking," International Journal of Bank Marketing, Vol. 30 No. 5, 2012. http://www.arvidhoffmann.nl/Hoffmann_Birnbrich_2012.pdf

Trusteer was acquired by IBM in 2013.

WGW03044-USEN-01