

2010 BiiB



Guardian Analytics and Ponemon Institute are pleased to present the results of the 2010 Business Banking Trust Study. ~~with~~

~~with~~ The data from this February 2010 survey shows criminals are successfully attacking small and medium business (SMB) bank accounts at an unprecedented rate, banks are failing to catch fraud and stop financial losses, and customers are losing trust in their institutions. Customers and banks are clearly out of alignment regarding responsibility for protecting online accounts and a staggering number of SMBs are firing their banks because of fraud.

The State of Business Banking Fraud

In 2009, fraud attacks on online business banking escalated so rapidly and with such staggering losses that the FBIⁱ and FDICⁱⁱ were moved to issue multiple warnings of the dangers of online banking. Well-funded cyber criminals executed a full-scale assault on authentication, leveraging widespread infection of end-user computers with banking trojans to sneak into online banking accounts completely undetected. Additionally, they perfected methods of moving large sums of money out undetected via wire, ACH, and bill pay, often resulting in six and seven figure fraudⁱⁱⁱ. It is expected to get worse before it gets better.

The national press has covered some of the largest and most prominent attacks, particularly those tied to lawsuits. But there has been no further investigation into the general scope and cause of fraud, nor the ongoing and bigger-picture impact a fraud attack of any size has on banks and small businesses.

The 2010 Business Banking Trust Study provides insights on the pervasiveness of fraud, the poor state of security at banks and businesses, and the destructive impact fraud has on businesses' relationships with their banks. More than 500 respondents from small and medium businesses representing many industries and geographical locations across the United States participated in the February 2010 study, conducted by independent research firm Ponemon Institute.

Executive Summary

The study's results send a clear message: Business banking across the country is under attack, but banks are failing to protect their customers' money. Small businesses cannot afford the time or money loss from a fraud attack and will move their business out of financial institutions that are not updating their security strategies to meet today's threats.

In 80% of fraud attacks, banks failed to identify the fraud before money left the institution.

Key highlights from the results include:

- **Fraud is more widespread than anticipated.** More than half of the respondents (55%) experienced a fraud attack in the last 12 months, 58% of which was enabled by online banking. More than half of those respondents experienced multiple attacks.
- **Banks are failing to detect fraud when it matters most – before money leaves the bank.** In 80% of the cases, banks failed to discover fraud prior to a transaction. This puts banks and businesses in an unproductive and contentious position of investigation, asset recovery and reimbursement negotiations.
- **Lack of ability to proactively identify fraud leads to financial losses.** In 87% of fraud cases, banks were unable to fully recover funds. This leaves banks and businesses the unpleasant and relationship-straining task of negotiating reimbursement.
- **Businesses are bearing the weight of losses with the banks.** In 57% of cases, businesses were not fully compensated for their losses, with 26% not compensated for any part of their losses.
- **Customer trust is fragile and easily broken, resulting in high rates of customer churn.** 40% of businesses that experienced fraud moved their business banking activities elsewhere after a fraud incident. 11% of these businesses terminated their banking relationship outright and 29% moved their primary cash management services to another bank.
- **Churn is driven by more than financial losses.** SMBs view productivity loss as the most serious consequence of bank-related fraud or attempted fraud (69%). Concern over unrecovered monetary assets was a close second (64%), followed by loss of reputation or goodwill with merchants, suppliers or vendors (47%).
- **Customers and banks are out of alignment regarding responsibility for security.** 67% believe their bank is ultimately responsible for protecting their accounts, but only 30% feel their bank is very safe in protecting their accounts from criminal attack and fraud.

Conclusions and Opportunities for Financial Institutions

According to the results, service, security and convenience are the three most important elements to small businesses in choosing a financial institution. While the data shows banks are in trouble with their customers, it also points to very specific opportunities to enhance security, service and convenience and build long-term, high value relationships with cash management clients.

1. Banks are unnecessarily exposing themselves to risk and need to change their perceptions of “reasonable security”. Think of “reasonable protections” not as the minimum required to avoid penalties or legal repercussions, but as the means to help prevent fraud attacks and customers from churning. Invest in people, process and technology to monitor transactions and identify the business banking customers with the highest risk of fraud before funds transfer. This approach will reduce productivity loss, profit loss, legal risk and reputation risk associated with navigating detailed fraud investigations, asset recovery and potential lawsuits. Security and customer trust is not an area to be penny-wise and pound-foolish.

2. Create a layered security strategy and evaluate solutions that will help deliver on proactive security AND customer convenience without overburdening IT staff. No one solution can solve the fraud problem, and experts recommend a layered approach using transaction monitoring solutions that complement existing security solutions. Institutions should look for approaches that can maximize detection with minimal false positive alerts. Solutions that use predictive analytics to evaluate every user’s online session to distinguish between legitimate and fraudulent activity provide high degrees of protection without overburdening IT staff. Predictive analytics-based solutions are also transparent to end users, providing protection without intruding on how customers log in or the requirements to complete a transaction.

3. It is unreasonable to put the burden of protection on SMBs. Fraudsters are directly targeting business customers with carefully crafted spear-phishing attacks. Executives are not clicking on amateur text e-mails from their personal accounts, but rather are tricked by sophisticated designs that look exactly like e-mails from the IRS, FBI, FDIC, ABA and related institutions.

End-point focused solutions, such as anti-virus, anti-malware and secure clients cannot keep up with the rapidly evolving banking Trojan landscape. In fact, even computers with updated anti-virus software can be infected with banking Trojans that allow fraudsters undetected access to accounts. Making matters worse, 75% of respondents access accounts from remote locations, including their home offices and 23% access accounts from their mobile devices. Business executives are accessing their company’s bank accounts from multiple locations and devices, demonstrating that they want to bank anytime, anywhere.

Properly securing all of these endpoints, and even the ones in the formal office, is almost impossible. Banks should assume, with the level of infection reported on end-user computers, that strong authentication solutions are no longer a means to keep fraudsters out.

4. Use your proactive efforts as a way to make customers feel safer and more confident in your ability to protect their information and their assets. 8% of respondents with a fraud attack actually felt the experience increased their trust in their bank. Based on this, there is opportunity to turn a potential negative, if caught in time, into a positive relationship-building experience. Unfortunately, banks find the attack before the transaction in only 20% of cases, and further, customers rated responsiveness from their banks following an attack as poor. In 40% of the incidents, their bank had not contacted the SMB within one week following the fraud.

5. Increase communication and transparency about your fraud and security policies. In the survey, 24% claim that their banks do not provide a policy explaining the bank's responsibilities to secure and protect their companies' accounts from fraud and 39% are unsure if such a policy exists. Clarity and expectations are pivotal to successful relationships. Take the time to ensure your customers know your policies and understand how you are protecting them.

About Guardian Analytics

Guardian Analytics is a pioneer in predictive analytics-based fraud prevention software for financial institutions. The company's FraudMAP® for Retail Banking and FraudMAP for Business Banking helps leading financial institutions proactively identify account compromise and stop fraud before a transaction occurs. FraudMAP creates a model of every online user's behavior and then, using Dynamic Account Modeling monitors every online session to determine the risk of online account takeover.

To learn more, visit www.guardiananalytics.com.

About Ponemon Institute

The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries. To learn more, visit www.ponemon.org.

ⁱ FBI Alert, Fraudulent Automated Clearing House (ACH) Transfers Connected to Malware and Work-at-Home Scams, Oct 2009

ⁱⁱ FDIC Special Alerts, August and October 2009

ⁱⁱⁱ Washington Post, Security Fix – Small Business Victims, 2009

^{iv} Trusteer, Measuring In the Wild Effectiveness of Antivirus against Zeus, September 2009