

## Case Study – Banking Industry Executive Level Financial Fraud



### Case Study – Digital Forensics

### Case Type – Internal Corporate Fraud

### Environment – Complex Multi-Location Network and Desktop computer forensics

### Industry – Banking

### Scenario:

A large accounting firm was hired to audit certain activities related to loans to individuals on the Board of Directors of a medium size, publicly traded bank (the “Bank”). During the Audit, the auditors needed to examine several computer systems used by certain Bank employees as well as by certain Board Members. GDF’s digital forensic examiners were immediately dispatched and sent in to arrange for the forensic analysis of the computer systems and to search for corroborating evidence in support of the audit team’s suspicions and findings. The systems GDF analysts forensically analyzed included laptop computers issued to managers in the loan origination department, desktop systems used by managers and board members. Email (Exchange) servers as well as Voicemail Systems were examined.

### Background Information:

In the previous two years, the Bank had gone through a series of transitions, culminating in a new Board of Directors and, because of new regulations in the financial industry, an independent Auditing Committee was appointed. The Auditing Committee charged certain officers of the Bank with engaging in suspect activities related to particular Bank expenses and loans that were either hidden or “lost” from the purview of the normal Bank’s accounting practices. In order to stay compliant and to remedy what may have been “bad apples” in the organization, the Bank’s Auditing Committee required the Board to hire an independent accounting firm to review those issues and present a formal report to the Bank. Because of the immense time pressure to solve those issues before the Bank was to release its next mandatory financial statement, a concise but thorough plan for reviewing expense and loan records as well as applications, approval processes and a multitude of other financial data stored in electronic as well as paper form. There was also an enormous volume of paper documents that the accounting firm was reviewing and needed to validate and review those documents against information gleaned from the digital examination as well. Because of the Bank’s

**Toll Free: 1-800-868-8189**  
**Int. Phone: Phone 727-287-6000**  
**<http://www.evestigate.com>**

size and market capitalization, it did not allocate surplus funds for this type of situation and cost factors were in the forefront, but could not guide the investigation on any substantive level for fear of bias and a lack of diligence.

### **GDF Involvement:**

Immediately upon being retained GDF analysts reviewed the computer systems with the banks IT department. After meeting with the audit committee and determining the focus of the audit and what was available in paper versus electronic GDF analysts work with the auditors to design a methodology that allowed for an in-depth forensic analysis of the electronic data and documents that virtually eliminated duplication of efforts by the forensic accountants by providing them with data and reports in electronic format that could be easily reviewed and audited.

GDF analysts were also able to utilize Computer Forensic Techniques to recover digital artifacts from the laptops and desktops of the suspect bank employees and board members. These forensic artifacts included email and documents exchanged through various free web based email accounts. These accounts were used to send and receive information on several mortgages and loans that were approved for “friends of the bank” that would normally have been denied or issued at a substantially higher interest rates.

### **GDF Findings:**

GDF focused a portion of its initial examination on particular desktop and network systems used by the suspect employees. Its examiners performed computer forensic analyses on those systems while simultaneously examining data supplied directly from the Bank’s IT department regarding internal network and Internet related activity of those suspect employees. Through those examinations, GDF forensically extracted digital artifacts, such as deleted email and documents and created reports of particular areas of interest based upon the issues related to the overall investigation. Using that collected information, the accounting firm was able to corroborate particular aspects of their investigation to conclude that certain Bank officers did in fact alter information supplied by certain loan applicants and influence approvals by bank employees for loans and expenses that fell well outside the banks normal approval criteria. Moreover, GDF also uncovered certain activities of the suspect employees that the auditors did not suspect, but which nevertheless, played an important role in the overall investigation and the final outcome.



**Toll Free: 1-800-868-8189**  
**Int. Phone: Phone 727-287-6000**  
**<http://www.evestigate.com>**

The reports and forensic analysis of the data from the banks internal banking systems including SunGard systems, internally developed applications and commercially available banking applications on a the distributed platforms (servers) and on the banks Unisys Mainframe allowed the audit team and forensic accounts to gather and analyze data in streamed lined and efficient manner. In fact, GDF was able to generate non standard reports and use data obtained from the Unisys and database logs to show how the internal controls were circumvented and by what users of the system. None of this information was available from standard reports saved valuable and expensive hours if the information had to be recreated from other data sources.

### **Outcome:**

Using the digital artifacts GDF collected in a forensically sound manner from the systems it investigated, the Bank's Auditing Committee was in a better position to find that certain Bank employees had violated Bank policy and possibly certain federal regulations regarding actions by officers of public corporations. The Auditing Committee and forensic accountants, together with the Bank's New Board of Directors, was able to terminate some of accused employees and also to negotiate settlement agreements favorable to the Bank with those employees, including reducing certain benefits and severance packages owed to them under pre-existing employment agreements.



The Bank was also able to call certain high risk loans and negotiate higher interest rates and better payment terms with the suspect loans reducing the banks risk and benefiting shareholders of the bank and bringing the bank into compliance thus reducing exposure to severe penalties and negative publicity.

In the end, the Bank saved an enormous amount of money and time by having the digital evidence to use in finalizing the issues related to the investigation and was able to make important deadlines with regards to certain SEC filings and regulatory mandates.

**Toll Free: 1-800-868-8189**  
**Int. Phone: Phone 727-287-6000**  
**<http://www.evestigate.com>**