FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

Deloitte Forensic Data Capture Services (Deloitte)

January 2013

FDIC External Service

Table of Contents

System Overview

When a financial institution fails, the FDIC, in its Receivership capacity, is responsible for conducting an investigation to determine the causes of the institution's failure. If necessary, the FDIC may also take legal action against the bank directors, officers, attorneys, accountants, and other "Persons-of-Interest" (POIs) who may have committed crimes or other breached their duties to the failed institution. Within FDIC, the Division of Resolutions and Receivers (DRR) works closely with the Legal Division to launch such investigations immediately after the closing of a failed institution. As part of each investigation, the DRR Investigations Group is responsible for gathering evidence to pursue professional liability claims[1] against POIs. In cases involving criminal activity, DRR and Legal staff coordinate with the FDIC Office of Inspector General (OIG) to conduct the investigations.

To support such investigations, FDIC has retained the services of Deloitte, LLP ("Deloitte Forensic Data Capture Services") to provide forensic data capture services during the resolution of failed institutions. At the direction of FDIC, the Deloitte Forensic Data Capture personnel travel to the failed bank site to locate, collect, and preserve[2] targeted digital data (i.e., email, electronic documents, database records, computer files, etc.) of identified POIs for analysis by DRR Investigations, Legal, and OIG staff. The Deloitte Forensic Data Capture staff collect digital data from two primary failed institution (FI) sources:

- FI Network Asset Collections (i.e., user email, user share, and department shares)
- FI User Asset Collections (i.e., hard drives of bank-owned laptops and desktops; bank-issued PDAs, Blackberry devices and cellphones, and external storage devices, such as USB drives, thumb drives, CDs, DVDs, etc.)

The captured digital information may include various types of sensitive information (SI) and personally identifiable information (PII) maintained by or pertaining to Persons-of-Interest (POIs). Additionally, the data could potentially include sensitive PII about bank customers and borrowers, such as deposit or loan information containing Social Security Numbers (SSNs).

Abiding by strict chain-of-custody, quality control, and on-site privacy/security procedures[3], the Deloitte Forensic Data Capture personnel securely extract, scan, and load the captured digital data onto encrypted hard drives and perform quality control[4] checks to verify the integrity of the captured data. The Deloitte Forensic Data Capture staff then securely ship one of the encrypted drives (i.e., the working copy) to Deloitte's primary forensic lab; the master copy is shipped to Deloitte's secondary forensic lab as a quality control procedure. At the primary Deloitte site, a standardized process is used for creating copies of forensic data on encrypted hard drives. The encrypted drives with copies of the forensic data are sent securely by courier to FDIC's Data Management Services (DMS) Vendor's Secure Data Center for loading to the DMS system. The original and working drives are securely shipped

[1] A professional liability clam is a type of Receivership claim pursued under civil law for losses caused by the wrongful conduct of directors, officers, lawyers, accountants, and others who are suspected of breaching their duty to a failed institution.
[2] Deloitte utilizes industry-standard forensic tools, technologies (e.g., EnCase), and methodologies to securely capture and preserve the digital data.
[3] Deloitte has gone through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to verify their having appropriate physical, technical and administrative security measures to safeguard FDIC-provided PII and other sensitive data.
[4] The quality control checks performed by Deloitte involve running a "MD5 Hash and Bit" stream file, but no data is accessed or retained as part of this process. MD5 is a cryptographic hash function, or algorithm, that maps large data sets of variable length, called keys, to smaller data sets of a fixed length. Cryptographic hash functions have many information security applications, notably in digital signatures and other forms of authentication. They can also be used as ordinary hash functions to index data, to detect duplicate data or uniquely identify files, and to detect accidental data corruption.

to a Records Management and Storage Vendor Facility for retention in accordance with FDIC policies.

Personally Identifiable Information (PII) in Deloitte

The data captured by the Deloitte Forensic Data Capture staff may contain various types of SI and PII pertaining to and/or maintained by POIs on the failed bank's systems, file shares, bank-issued devices, etc. In addition, the data may potentially contain sensitive PII about bank customers and borrowers in instances where loan or deposit data is captured as part of the POI investigation. Specific types of PII may include: full name, date of birth (DOB), place of birth, SSN, employment information, mother's maiden name, official certificates (i.e., birth, death, naturalization, marriage, etc.), medical information, home address, phone numbers, email address, financial information, driver's license information, vehicle identifiers (i.e., license plates), photographic identifiers, military records, and investigation reports.

Purpose & Use of Information in Deloitte

After securely receiving a list of POIs from FDIC DRR Investigations staff, the Deloitte staff search and forensically capture targeted electronic data pertaining to POIs from the institution's databases, email servers, file servers, bank-issued equipment (i.e., PDAs, cell phones, laptops, etc.), and other failed institution sources. This captured electronic data, which contains PII and SI, is necessary to support the pursuit of criminal and/or professional liability claims against POIs.

Sources of Information in Deloitte

When a financial institution closes, the FDIC DRR Investigator-in-Charge (IIC) securely provides the Deloitte Forensic Data Capture personnel with a list of POIs who are the subjects of FDIC civil and/or criminal investigations. The Deloitte staff electronically search failed financial institution sources to identify and capture digital data pertaining to POIs. These sources may include bank-owned computer hard drives, email services, file servers, bank-issued PDAs, Blackberry devices, cellphones, external storage devices, and any other electronic back-up locations as directed by the FDIC.

Notice & Consent

Individuals do not have the opportunity to opt out of providing their data or consenting to particular uses of their information. All information is obtained directly from failed financial institutions and is necessary to support the FDIC's investigation into the cause of the financial institution's failure.

Access to Data in Deloitte

Authorized FDIC OIG, DRR, and Legal Division staff have access to the forensic data captured by Deloitte via FDIC's Data Management Services (DMS) system in support of their investigation into the cause of an institution's failure. Authorized DRR and Legal Division contractors who support FDIC employees in investigating bank failures and pursuing civil and criminal claims also have access to the forensic data maintained in the FDIC's DMS system. In certain instances, it may be necessary for the Deloitte Forensic Data Capture staff to provide copies of the unaltered forensic data to FDIC staff in accordance with contractual requirements and upon written request from FDIC. In such instances, the Deloitte staff create copies of the data in Deloitte's secure forensic lab and securely send the copies of the requested data on encrypted hard drives to the authorized FDIC requestor.

Authorized Deloitte staff and subcontractors have access to the PII collected as part of providing forensic data capture and information technology support services to the FDIC during the resolution of a failed institution. Access to this data is limited to those with a "need to know," and Deloitte takes full responsibility for the conduct of its subcontractors to ensure the confidentiality, integrity, and availability of the sensitive information collected and maintained by Deloitte.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

The Deloitte Forensic Data Capture does not involve directly uploading or providing the captured forensic data to any internal FDIC system/application or any external non-FDIC system/application.

System Name	System Description	Type of Information Processed
N/A	N/A	N/A

Data Accuracy in Deloitte

Data is collected directly from failed financial institutions. As such, the FDIC and the Deloitte Forensic Data Capture Services staff rely on the financial institutions to provide accurate data. Deloitte performs quality control checks to verify the integrity of the data.

Data Security for Deloitte

Access to the forensic data captured from the failed financial institution is limited to individuals with a "need-to-know" the information for performing their job duties. In addition, it is every FDIC's user's responsibility to abide by FDIC data protection rules. All sensitive data and PII is shipped securely and in accordance with established FDIC privacy and security policies and guidelines.

Per its contractual agreement with FDIC, Deloitte assumes full responsibility for the conduct of its subcontractors to ensure the confidentiality, integrity, and availability of the sensitive information collected and maintained by Deloitte. Deloitte has completed the security

review required by the FDIC to determine and verify that they have the appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data.

System of Records Notice (SORN)

The Deloitte Forensic Data Capture Services operates under the FDIC Privacy Act SORN 30-64-0013, *Insured Financial Institution Liquidation Records*.

Contact Us

To learn more about the FDIC's Privacy Program, please visit: http://www.fdic.gov/about/privacy/.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the FDIC Privacy Program Contacts. You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.