# PUBLICATION

## Case Study of a CFPB Enforcement Action: In re JPMorgan Chase Bank, N.A.; and Chase Bank USA, N.A.

**December 19, 2013**

The Consumer Financial Protection Bureau (CFPB) brought an enforcement action against JPMorgan Chase Bank, N.A. and Chase Bank USA, N.A. (collectively, the Bank), pursuant to 12 U.S.C. §§ 5563 and 5565 with regard to their billing and administration of identity protection products. Specifically, it alleged that the Bank had billed customers for credit monitoring and credit protection services that were not, in fact, provided. The Bank agreed to the issuance of a consent order, pursuant to which the Bank agreed to (a) design and implement various policies and procedures to correct the issue, and to not market any identity protection products until such policies and procedures have been submitted to and approved by the CFPB; (b) make restitution of all amounts illegally charged; and (c) pay a civil monetary penalty of $20 million to the CFPB.

### Findings

From October 2005 to March 2012, the Bank and its vendors marketed, offered for sale and sold identity protection products that purported to monitor customers' credit information in order to alert them to activity that would indicate identity theft or other fraudulent use of their financial information. The Bank represented that, in exchange for a monthly fee, the Bank and/or its vendors would provide features that included a product named "3-CFPB Credit Monitoring." This product was to provide daily monitoring of customers' information at three credit reporting agencies to identify and alert customers to activity that could suggest fraudulent use of their identities. These products were sold as "add-on" features to new or existing credit card accounts, as well as to retail bank customers and non-customers. Once the customer was enrolled in the program, the servicing of the identity protection product was delegated by the Bank to Corelogic, Inc. Corelogic was formerly known as First Advantage Membership Services, Inc. for Chase Fraud Detector, True Credit for the Chase Identity Protection, and Intersections, Inc. for Chase Identity Protection.

Pursuant to the Fair Credit Reporting Act (FCRA), Corelogic provided customers with the materials necessary to grant it authorization to access their credit information from the reporting agencies in order to activate "3-CFPB Credit Monitoring." In many cases, however, the CFPB found that some period of time passed before customers provided authorization, or that Corelogic never obtained the authorization. In still other cases, customers provided authorization, but one or more credit reporting agencies would not process it for various reasons. These issues were not caught by the Bank's compliance monitoring, service provider management or quality assurance methodologies. As a result, though the Bank and Corelogic were unable to activate the "3-CFPB Credit Monitoring," those customers were nonetheless billed for those services that were not provided. The pool of customers affected by this error exceeded 2.1 million customers, who were billed least $270 million in fees and over-limit charges, as well as more than $39 million in associated interest fees.

### Resolution

The Bank and the CFPB agreed to the issuance of a consent order, pursuant to which the Bank was ordered to do the following:

- Cease and Desist – The Bank is barred from marketing, soliciting, offering for sale and selling its "Chase Identity Protection" and "Chase Fraud Detector" products, until such time as it submits a Compliance Plan to the CFPB.
- Action Plan – On or before December 18, 2013, the Bank was to submit an Action Plan to the CFPB to address the actions "necessary and appropriate to achieve compliance" with the order, including the development or revision of a written Vendor Management Policy, which must require (a) a written contract between the Bank and its vendor, setting forth the rights and responsibilities of each with respect to the identity protection products; (b) an analysis to be conducted by the Bank prior to contracting with a vendor for services related to the identity protection products; and (c) periodic onsite review by the Bank of the vendors controls, performance and information systems.
- Unfair, Deceptive or Abusive Acts or Practices (UDAAP) Policy – On or before December 18, 2013, "an appropriate independent qualified group within the Bank" must develop a UDAAP policy for any add-on products, that shall require:

  - Annual written review of any changes to policies and procedures affecting add-on products considered to be high risk for UDAAP, as well as of any new products considered to be at high risk for UDAAP.
  - Recording of all telephone marketing or sales calls *by either the Bank or the vendor*, with the recordings to be retained for a period of at least 25 months from the date of the call.
  - Recording of all telephone calls *by either the Bank or the vendor* with enrolled customers in which the customer indicates that he or she did not authorize, does not want or need, or wishes to cancel the product, with the recordings to be retained for a period of at least 25 months from the date of the call.
  - "Comprehensive" written procedures for training Bank employees and vendor call agents on applicable Federal consumer financial laws and the Bank's policies and procedures regarding telephone calls with customers regarding the products, as well as for Bank and vendor employees who monitor such calls.
  - "Comprehensive" written policies and procedures for identifying and reporting violations of applicable Federal consumer financial laws and the Bank's policies and procedures, by the Bank's employees and vendor's employees or agents, in a "timely" manner.
  - "Independent" call monitoring by "qualified" personnel.
  - Written policies and procedures to ensure that the risk management, internal audit and corporate compliance programs have the "requisite authority and status" within the Bank to identify and remedy deficiencies.
- Consumer Compliance Internal Audit Program – On or before December 18, 2013, the Bank was to develop and submit a written internal audit compliance program to the CFPB Regional Director, which must include:

  - Written policies and procedures for conducting audits of the Bank's compliance with applicable Federal consumer financial laws.
  - Written policies and procedures for expanding the sampling of the internal audit when exceptions based on potential violations are detected.
- Redress – On or before November 18, 2013, the Bank was required to develop a redress plan for making full restitution to all affected customers of all monthly fees paid for the identity protection products, all over-limit fees paid due to the charging of the monthly fees, and all finance charges accrued on the monthly fees, minus any redress already made, and submit it to the Regional Director for review and non-objection.
- Civil Monetary Penalty – On or before September 29, 2013, the Bank was to pay a civil fine in the amount of $20 million to the CFPB, with such penalty not to be treated as an offset, deduction or

credit against any federal, state or local tax or fine, or against any court judgment. The Bank is also barred from seeking indemnity from any applicable policy of insurance to recoup this amount.

**Why This Matters**

The significance of both this enforcement action and the manner of its resolution is that they highlight the scope of liability and increased scrutiny that the CFPB intends to apply to consumer credit products. In particular, going forward, the CFPB clearly expects a high degree of transparency as to consumer communications with banks and their third-party vendors regarding credit protection and other "add-on" products, holding banks more to account for the acts and omissions of those vendors, and contemplates a much closer, almost "hand-in-glove," relationship between the CFPB's regional directors and the banks that they supervise. The regime mandated by the consent order seeks a much less flexible, more extensive internal and external compliance structure for banks and mortgage servicers, coupled with more rigorous record-keeping and record-retention formulae for communications with customers. This also appears to assume and require a relatively high degree of compliance training for everyone from the call agent on through the ranks who is in any way involved with marketing, selling or servicing credit protection products. All told, if this action is emblematic of the future relationship between the CFPB and regulated financial institutions, it represents a paradigm shift in how the financial industry operates, and predictably will result in markedly increased overhead.