February 28, 2020

District Court Finds Phishing Scheme Not Covered "Forgery" Under Financial Institution Bond

BY: Jason Taylor

In *Crown Bank JJR Holding Company, Inc. v. Great American Insurance Company,* 2020 WL 634147 (D.N.J. Feb. 11, 2020) a New Jersey federal court found that forgery coverage under a Financial Institution Bond was not triggered where funds were wired as a result of an email phishing scheme. The court, however, held that the record was insufficient to determine whether or not coverage might apply under a "Computer Systems Fraud" Insuring Agreement.

Crown Bank JJR Holding Company, the insured, provides its customers with the ability to submit requests for wire transfers by phone or email. When this process is initiated, Crown Bank requires its employees to request a signed wire transfer authorization form from the customer and to call the customer for confirmation that the signature on the authorization form is valid. Jacinto Rodrigues, the Chairman and CEO of Crown Bank, and his wife, Joaquina, a director of Crown Brank had a number of personal and business accounts at Crown Bank. Crown Bank also kept copies of the Rodrigueses signatures on file.

For approximately three weeks in April 2012 Crown Bank received thirteen wire transfer requests purportedly from Mrs. Rodrigues. The requests were sent from an email address, "jackiiesumo@gmail.com," which was almost identical to one used by the real Mrs. Rodrigues, but with the addition of a second lowercase "i". The requests all asked for wire transfers to a bank in Singapore.

Upon receipt a Crown Bank employee requested the necessary information to complete the transfers. Completed wire transfer authorization forms were then sent to the email claiming to be Mrs. Rodrigues, and the person on the other end of that email address would send the forms back with a signature that matched the signature Crown Bank had on file. The employees printed off the forms to confirm the signatures were a match, and twelve of the thirteen requests were processed without the employee calling Mrs. Rodrigues to confirm the requests. When the employee received a thirteenth request for three additional transfers to the Singapore bank, he called Mrs. Rodrigues to confirm the requests. Upon learning about the phishing scheme, Mrs. Rodrigues executed an affidavit of forgery for each completed transfer. Crown Bank had wired just over $2.7 million of the Rodrigueses funds before the scam was discovered.

Crown Bank sought coverage under the Financial Institution Bond, which covered "Loss resulting directly from the Insured having, in good faith, paid or transferred any Property in reliance on any Written, Original … (4) Withdrawal Order [or] … (6) Instruction or advice purportedly signed by a customer of the Insured or by a banking institution …which (a) bears a handwritten signature of any maker, drawer or endorser which is Forgery; or (b) is altered, but only to the extend the Forgery or alternation causes the loss. The Insuring Agreement also required that actual physical possession of the items listed above by the Insured is a condition precedent to the Insured's having relied on the fraudulent items.

The policy went on to define “Original” as meaning “the first rendering or archetype and does not include photocopies or electronic transmissions even if received and printed.” The dispute between the parties was whether Crown Bank satisfied the condition precedent to coverage by being in actual, physical possession of the “Original” wire transfer forms.

Crown Bank argued that the PDF documents themselves could be considered “Originals” based on two theories: (1) that the forms were printed out by the employees to verify the signatures and (2) a PDF could be considered a “first rendering or archetype” and any ambiguity in those words should be construed in favor of the insured.

The court disagreed and explained that the first theory was “simply contrary to the express language of the FIB” which stated that electronically transmitted documents are not originals, “even if received and printed.” The second theory also failed as the electronic transmission language in the policy voided any potential argument about the classification of the PDF. The court reasoned that any ambiguity in the “first rendering or archetype” classification of a PDF was unimportant, because the PDF being transmitted electronically meant it cannot be an “Original”.

Accordingly, the court found that Crown Bank failed to meet a condition precedent for coverage, and, therefore, the phishing scam did not implicate the Policy’s forgery coverage.

The court used similar reasoning to find that Crown Bank was not entitled to coverage under a Rider providing additional coverage under the Financial Institution Bond. The Rider amended Insuring Agreement D for forgery or alteration by adding the following:

"Loss resulting directly from the Insured having accepted, paid or cashed any check or withdrawal order made or drawn on a customer’s account which bears the signature or endorsement of one other than the person whose name and signature is on file with the Insured as signatory on such account, shall be deemed to be a Forgery under this Insuring Clause. It shall be a condition precedent to the Insured’s right of recover under this coverage that the Insured shall have on file signature of all persons who are signatories on such account."

Crown Bank argued that coverage was triggered because Mrs. Rodrigues executed an affidavit of forgery and the signature on the forms was of someone other than Mrs. Rodrigues. The court, however, rejected that argument because the record clearly indicated that Crown Bank “repeatedly conceded that each of the wire transfer forms bore ‘Mrs. Rodrigues’s signature.’” Moreover, the court reasoned that the Rider did not vary any term or limitation of the bond, and possession of the “Original” was still a condition precedent of coverage. As previously held by the court, Crown Bank did not have possession of the “Original” wire transfer forms and would not be entitled to coverage.

Not all was lost for the insured. Crown Bank also sought coverage under the “Computer Systems Fraud Insuring Agreement” under a Computer Crime Policy which covered, in relevant part, “Loss” resulting directly from a fraudulent (1) entry of Electronic Data or Computer Program into, or (2) change of Electronic Data or Computer Program within any computer system operated or used by the Insured; provided the entry or change causes an account of the Insured, or of its customer, to be added, deleted, debited or credited. The court, however, determined that without further information the record was insufficient to determine the extent of coverage under CSFIA. The court requested additional, expedited briefing on the issue.