UNITED STATES OF AMERICA
BEFORE THE
COMMODITY FUTURES TRADING COMMISSION AM 11: 12

In the Matter of	:	**CFTC Docket No. 09-11**
Interbank FX, LLC,	:	**ORDER INSTITUTING PROCEEDINGS PURSUANT TO SECTIONS 6(c) AND 6(d) OF THE COMMODITY EXCHANGE ACT AND MAKING FINDINGS AND IMPOSING REMEDIAL SANCTIONS**
Respondent.	:	

I.

The Commodity Futures Trading Commission (the "Commission") has reason to believe that Interbank FX, LLC ("Interbank"), a registered futures commission merchant ("FCM"), has violated Commission Regulations 160.5, 160.10 and 160.30, 17 C.F.R. §§ 160.5, 160.10 and 160.30 (2008), promulgated pursuant to Sections 5g and 8a(5) of the Commodity Exchange Act, as amended, 7 U.S.C. §§ 7b-2 and 12a(5) (2006). Therefore, the Commission deems it appropriate and in the public interest that public administrative proceedings be, and they hereby are, instituted to determine whether Interbank engaged in the violations set forth herein, and to determine whether an order should be issued imposing remedial sanctions.

II.

In anticipation of the institution of this administrative proceeding, Interbank has submitted an Offer of Settlement ("Offer"), which the Commission has determined to accept. Without admitting or denying any of the findings and conclusions herein, Interbank acknowledges service of this Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act and Making Findings and Imposing Remedial Sanctions ("Order").[1]

[1] Interbank consents to the entry of this Order, and the use of these findings in this proceeding and in any other proceeding brought by the Commission or to which the Commission is a party; provided, however, that Interbank does not consent to the use of the Offer, or the findings or conclusions consented to in this Order, as the sole basis for any other proceeding brought by the Commission, other than a proceeding in bankruptcy or to enforce the terms of this Order. Nor does Interbank consent to the use of this Order, or the findings or conclusions consented to in the Offer or this Order, by any other party in any other proceeding.

III.

The Commission finds the following:

A. Summary

In March 2008, Interbank discovered that one of its Information Technology ("IT") employees had placed files containing confidential personal customer information such as, names, addresses, phone numbers, dates of birth, social security numbers, passport numbers, drivers license numbers and bank account numbers ("personal identifying information" or "PII") of approximately 13,000 customers or potential customers on a personal website that was accessible on the Internet. The information was accessible for at least a year. The firm did not have effective procedures in place to prevent its employees from handling PII in this manner, which led to the inadvertent disclosure of such information on the Internet. Accordingly, Interbank has violated Commission Regulations 160.5, 160.10 and 160.30, 17 C.F.R. §§ 160.5, 160.10 and 160.30 (2008).

B. Respondent

Interbank FX, LLC is an active domestic limited liability company organized in Utah on November 26, 2002 with its principal place of business at 365 E. Millrock Drive, Suite 200, in Salt Lake City, Utah. It conducts retail foreign currency trading and became registered with the CFTC as a futures commission merchant on December 23, 2004 and is also a forex dealer member of the National Futures Association ("NFA").

C. Facts

1. The Security Breach Incident.

Starting in the fall of 2006 as part of an effort to enhance the security of its data and computer network, Interbank began the process of splitting its computer server into a production (or "live") server and a development server. A software engineer employed by Interbank (the "Software Engineer") maintained and ran reports from an in-house database called the Interbank Customer Application Database ("ICAD"), a database that contained all the information from a customer's account application and thus contained sensitive information such as social security numbers, driver's license numbers, passport numbers, bank account numbers and net worth information. Before the split in the servers, the Software Engineer had access to the production server and made changes to ICAD or ran reports on the live data. After the split, the Software Engineer needed to work on a prototype of ICAD that he maintained on his computer and also needed access to live data to run reports. The Software Engineer found it more difficult to work in this environment and determined that he could not make some changes requested by Interbank on his work computer. Therefore, he asked an Interbank systems engineer (the "Systems Engineer"), who still had access to the production server, for copies of the ICAD database. The Systems Engineer copied the data requested onto the firm's shared file server and the Software Engineer transferred that data by file transfer protocol

("FTP") to his personal website, where he could more easily work with the data.[2] While Interbank does not know how many times he did this or when he started downloading PII, the files that Interbank found when it discovered the security breach were uploaded to the Software Engineer's personal website in February, March and April 2007.

On March 28, 2008, an Interbank customer discovered her PII on the Internet after conducting a Google search and reported it to Interbank. Interbank immediately began an investigation to determine how this information became available on the Internet and quickly learned that it originated from the Software Engineer's personal website. Then, Interbank hired expert consultants who determined that the files uploaded by the Software Engineer to his personal website included approximately 13,000 customer and prospective customer files. Interbank also contracted with Equifax to provide counseling and credit watch services for most of the affected customers. Finally, Interbank contacted the NFA and the CFTC about the situation and submitted to NFA for their review a notice to be issued to Interbank's affected customers.

2. Interbank's Lack of Effective Policies or Procedures to Safeguard Customer Records and Information

Interbank did not have policies or procedures directed to the protection of consumer PII in the winter or spring of 2007, when the Software Engineer uploaded the customer files later discovered by an Interbank customer.[3] Interbank drafted a series of procedures dealing with computer security issues after the spring of 2007, but none of them deal with the security of consumer PII. In April 2008, Interbank did take the step to encrypt PII, which should prevent an inadvertent disclosure of consumer PII in the future.

Despite a lack of effective procedures or policies, Interbank issued a Privacy Notice to its customers as early as December 23, 2004, which stated erroneously that Interbank "maintain[ed] physical, electronic and procedural safeguards that comply with federal standards to guard [customer] information."

---

[2] The Software Engineer also uploaded other Interbank data including information relating to Interbank's operation, a database used by Interbank IBs and a database used for demonstration accounts.

[3] Interbank did draft an Acceptable Use of Computer and Network Systems Policy and Network Security Policy in October and December 2006 respectively. These policies, however, only dealt with computer security at a macro level, and not PII specifically, and were enacted to protect the company from external threats and liability, not to protect consumer data. Moreover, there is no evidence they were implemented or enforced.

D. Legal Discussion

1. Interbank's Privacy Notice to Customers Did Not Accurately Reflect Its Privacy Policies and Procedures.

Commission Regulation 160.5 requires that all FCMs, commodity trading advisors ("CTA"), commodity pool operators ("CPO") and introducing brokers ("IB") subject to Commission jurisdiction provide a clear and conspicuous notice to customers that accurately reflects its privacy policies and practices not less than annually during the life of the customer relationship. Since at least December 2004, Interbank has provided an annual privacy notice to its customers that inaccurately stated that Interbank "maintain[s] physical, electronic, and procedural safeguards that comply with federal standards to guard [customer] personal information." Interbank, however, did not have any effective procedural safeguards to protect sensitive customer information and did not have any physical or electronic safeguards until after the Software Engineer put PII on a publicly available Internet website. Interbank has therefore violated Commission Regulation 160.5.

2. Interbank Disclosed Nonpublic Personal Information to Nonaffiliated Third Parties Without Notifying Its Customers.

Commission Regulation 160.10 provides that an FCM, CTA, CPO or IB may not, directly or through an affiliate, disclose any nonpublic personal information about a consumer[4] to a nonaffiliated third party unless it has provided the consumer an initial privacy notice, an opt-out notice, and a reasonable opportunity to opt out of disclosure and the consumer does not opt out. Interbank disclosed personal consumer information to a nonaffiliated third party (i.e. the Internet) and did not tell its customers or prospective customers it was doing so. It is therefore in violation of Commission Regulation 160.10.

3. Interbank Lacked Effective Procedures to Safeguard Customer Reports and Information.

Commission Regulation 160.30 provides that every FCM, CTA, CPO and IB must adopt policies and procedures that address the administrative, technical and physical safeguards for the protection of customer records and information. The policies and procedures must be reasonably designed to a) insure the security and confidentiality of customer records and information; b) protect against any anticipated threats or hazards to

---

[4] A consumer under Part 160 of the Commission's Regulations is an individual who obtains or has obtained a financial product or service from an FCM, CTA, CPO or IB that is to be used primarily for personal, family or household purposes. 17 C.F.R. § 160.3(h)(1) (2008). Consumers would include for example, individuals who provide nonpublic personal information to an FCM, CTA, CPO or IB in connection with obtaining or seeking to obtain brokerage or advisory services, whether or not the entity provides the services or establishes a continuing relationship with the individual. 17 C.F.R. §160.3(h)(2)(i). A customer is a consumer who has a continuing relationship with the FCM, CTA, CPO or IB. 17 C.F.R. § 160.3(k) (2008).

the security or integrity of customer records and information; and c) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. Interbank lacked effective procedures to protect customer records before the Software Engineer uploaded files containing sensitive customer information to his personal website. This failure is a violation of Commission Regulation 160.30.

E. Respondent's Remedial Efforts and Cooperation

The settlement in this matter takes into consideration the nature and extent of Interbank's remedial efforts and cooperation with the Commission. Upon learning of the incident on March 28, 2008, Interbank took immediate affirmative steps to investigate and determine the manner in which the PII was available on the Internet and to remove it from the website in question. By that night, Interbank had deleted all information from the Software Engineer's website and ensured that no Interbank derived customer information was available on any other website. Interbank also worked with Internet search engines to remove the website from the search indexes and to delete any records of the customer data. By March 30, 2008, neither the Software Engineer's website nor any trace of the Interbank derived customer information was available through any search engine or any other website.

Interbank conducted an internal investigation of the breach and also hired an expert consultant to determine the extent of the breach and to forensically secure the information for evidentiary purposes. Within a week of the discovery of the breach, Interbank self-reported it to the NFA and the Commission. On April 8, 2008, Interbank sent a notification letter to affected individuals in the United States, offering each the opportunity to enroll, for free, in a comprehensive credit monitoring and insurance program for one year. Shortly thereafter, Interbank had sent notifications to affected individuals outside of the United States, again offering similar credit monitoring services. It has terminated the employment of the Software Engineer who placed the PII on his personal website.

Interbank also has cooperated with the Commission's Division of Enforcement's ("Division") investigation of the breach. In the months following the discovery of the incident, Interbank presented the results of its internal investigation to the Division, kept the Division informed regarding its offer of credit-monitoring services to customers, and fully cooperated with the Division in its investigation, including the voluntary production of documents and witnesses.

The sanctions imposed by this Order take into consideration Interbank's remedial efforts and cooperation, as set forth above. Absent that cooperation, the Commission likely would have imposed a more severe sanction. The Commission has previously noted that it takes a respondent's level of cooperation into consideration in evaluating settlement offers. *See In re El Paso Merchant Energy, L.P.*, [2003-2004 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 29,431 (CFTC March 26, 2003) (respondent voluntarily provided results of internal investigation, which revealed violative conduct, to the

Commission.); *In re Sumitomo Corp.*, [1996-1998 Transfer Binder] Comm. Fut. L. Rep. (CCH) ¶ 27,327 (CFTC May 11, 1998) (respondent's cooperation included voluntary production of documents that the Commission might not have been able to obtain from a foreign corporation.)

IV.

FINDINGS OF VIOLATIONS

Based on the foregoing, the Commission finds that Interbank violated Commission Regulations 160.5, 160.10 and 160.30, 17 C.F.R. §§ 160.5, 160.10 and 160.30 (2008).

V.

OFFER OF SETTLEMENT

Interbank has submitted an Offer of Settlement ("Offer") in which it acknowledges service of this Order and admits the jurisdiction of the Commission with respect to the matters set forth in this Order and waives (1) the service and filing of a complaint and notice of a hearing; (2) a hearing; (3) all post-hearing procedures; (4) judicial review by any court; (5) any and all objections to the participation by any member of the Commission's staff in the Commission's consideration of the Offer, (6) any and all claims that it may possess under the Small Business Regulatory Enforcement Fairness Act, 1996 HR 3136, Pub. L. 104-121, §§ 231-232, 110 Stat. 862 (1996), as amended by Pub. L. No. 110-28, 121 Stat. 112 (2007), relating to, or arising from this proceeding; (7) any and all claims that it may possess under the Equal Access to Justice Act (EAJA), 5 U.S.C. § 504 (2006) and 28 U.S.C. § 2412 (2006), and/or part 148 of the Commission's Regulations, 17 C.F.R. §§ 148.1 et seq. (2008), relating to, or arising from this proceeding; and (8) any claim of double jeopardy based upon the institution of this proceeding or the entry in this proceeding of any order imposing a civil monetary penalty or any other relief. Interbank makes its offer of settlement without admitting or denying any of the findings and conclusions herein.

Interbank stipulates that the record basis on which this Order is entered consists of this Order and the findings in this Order consented to in the Offer. Interbank consents to the Commission's issuance of this Order, which makes findings as set forth herein and orders that Interbank: (1) cease and desist from violating the provisions of the Commission Regulations it has been found to have violated; (2) pay a civil monetary penalty in an amount of $200,000; and (3) comply with its undertakings as consented to in the Offer and set forth below in Section VI of this Order.

Upon consideration, the Commission has determined to accept Interbank's Offer.

VI.

ORDER

Accordingly, **IT IS HEREBY ORDERED THAT:**

A. Interbank shall cease and desist from violating Commission Regulations 160.5, 160.10 and 160.30, 17 C.F.R. §§ 160.5, 160.10 and 160.30 (2008);

B. Interbank shall pay a civil monetary penalty in the amount of $200,000 within 10 days of the date of the entry of this Order. Interbank shall pay its civil monetary penalty by electronic funds transfer, U.S. postal money order, certified check, bank cashier's check, or bank money order. If payment is to be made by other than electronic funds transfer, the payment shall be made payable to the Commodity Futures Trading Commission and sent to the address below:

Commodity Futures Trading Commission
Division of Enforcement
ATTN: Marie Bateman – AMZ-300
DOT/FAA/MMAC
6500 S. MacArthur Blvd.
Oklahoma City, OK 73169
Telephone 405-954-6569

If payment by electronic transfer is chosen, Interbank shall contact Marie Bateman or her successor at the above address to receive payment instructions and shall fully comply with those instructions. Interbank shall accompany payment of the penalty with a cover letter that identifies Interbank and the name and docket number of this proceeding. Interbank shall simultaneously transmit copies of the cover letter and the form of payment to (1) the Director, Division of Enforcement, Commodity Futures Trading Commission, 1155 21st Street, N.W., Washington, D.C. 20581; and (2) the Chief, Office of Cooperative Enforcement, Division of Enforcement, Commodity Futures Trading Commission at the same address. In accordance with Section 6(e)(2) of the Act, 7 U.S.C. § 9a(2) (2006), if this amount is not paid in full within 15 days of the due date, Interbank shall be prohibited automatically from the privileges of all registered entities, and, if registered with the Commission, such registration shall be suspended automatically until it has shown to the satisfaction of the Commission that payment of the full amount of the penalty with interest thereon to the date of the payment has been made; and

C. Interbank and its successors and assigns shall comply with the following undertakings as set forth in the Offer:

1. Interbank shall establish, implement and thereafter maintain a documented comprehensive security program to address administrative, technical and physical safeguards for the protection of consumer (as that term is defined in Commission Regulation 160.3(h)(1), 17 C.F.R. § 160.3(h)(1) (2008)) records and information, including:

a. Designating an employee or employees by either the board of directors or principals of the company to coordinate and be accountable for the program;

b. Identifying material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee and contractor training and management (service providers must be able to maintain the safeguards set forth in the security program); (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to internal security breaches, attacks, intrusions, or other systems failures;

c. Designing and implementing information safeguards to control the risks identified through the risk assessment described in paragraph 2 above, including but not limited to encrypting consumer data containing personal identifying information, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls and systems;

d. Evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances;

e. Ensuring at least annual appropriate security awareness training of all staff and contractors that includes an explanation of Interbank's policies and procedures for ensuring the safety of consumer records and information; and

f. Obtaining a written assessment and report (an "Assessment") from an objective, independent third-party professional qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); and who holds Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security Institute (SANS), using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after the date of entry of this Order, and annually thereafter for 5 years after the date of entry of this Order, that:

i. sets forth the specific administrative, technical, and physical safeguards that Interbank has implemented and maintained during the reporting period;

ii. explains if and how such safeguards are appropriate to Interbank's size and complexity, the nature and scope of Interbank's activities, and the sensitivity of the personal information collected from or about consumers;

iii. explains how the safeguards that have been implemented meet or exceed the protections required by Commission Regulation 160.30, 17 C.F.R. § 160.30 (2008); and

iv. certifies that Interbank's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected throughout the reporting period.

Immediately upon Interbank's receipt, Interbank shall send copies of these Assessments to the Regional Counsel, Division of Enforcement, Commodity Futures Trading Commission, 525 West Monroe Street, Suite 1100, Chicago, Illinois 60661; and

2. Neither Interbank nor any of its successors, assigns, employees, agents, or representatives shall take any action or make any public statement denying, directly or indirectly, any finding in the Order, or creating, or tending to create, the impression that the Order is without a factual basis; provided, however, that nothing in this provision affects Interbank's (i) testimonial obligations; or (ii) right to take appropriate legal positions in other proceedings to which the Commission is not a party. Interbank and its successors and assigns shall take all steps necessary to ensure that all of their employees, agents and representatives under their authority and/or actual or constructive control understand and comply with this undertaking.

The provisions of this Order shall be effective on this date.

By the Commission:

David A. Stawick

David A. Stawick
Secretary of the Commission
Commodity Futures Trading Commission

Dated: June 29, 2009.