

WRITTEN STATEMENT OF
BASSEM BANAFI
CPA, CFE, ABV, CGMA, CAMS, CFCS, CFF, EnCE
FINANCIAL FORENSICS CONSULTANT
BEFORE THE
U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

JANUARY 30, 2018

Madam Chairman, Ranking Member Green, and Members of the Subcommittee, thank you for the opportunity to testify before the Subcommittee on Oversight and Investigations.

My name is Bassem Banafa. I am a Financial Forensics Consultant and Expert Witness at my firm, Bassem Banafa, LLC, and for PlainSite, an organization that works on legal transparency, among other issues.

I previously served as a Forensic Accountant with the Special Operations Division of the Contra Costa County District Attorney's Office in Martinez, California. I assisted investigators and prosecutors with complex cases involving large-scale fraud, human trafficking, drug trafficking, money laundering, and other criminal activities. In those investigations, I personally reviewed tens of millions of dollars in transactions conducted by human trafficking organizations.

Prior to my time at Contra Costa, I served as a Financial Crimes Consultant with Wells Fargo's Financial Institution Investigations Group ("FIIG"). Wells Fargo created FIIG in response to the findings of a 22-month long investigation by the Drug Enforcement Administration, the Internal Revenue Service and other agencies regarding Wachovia's¹ handling of \$373 billion in wire transfers, \$47 billion in remote deposits², and nearly \$5 billion in bulk cash deposits processed on behalf of "Casas de Cambio," high-risk currency exchange businesses operating in Mexico. The investigation concluded that these transactions were conducted with limited or no anti-money laundering oversight by Wachovia and at least \$110 million of the funds processed were directly related to criminal drug trafficking activity.³ FIIG was tasked with investigating

¹ In 2008, Wells Fargo acquired Wachovia, knowing that the bank was being investigated for failures in its money laundering oversight. I understand that Wells Fargo cooperated with authorities throughout the investigation of Wachovia.

² Typically, a set of check images collected off-site and transmitted to the financial institution for processing. These types of transactions were used to disguise the parties to a transaction by presenting images, which require manual processing for anti-money laundering analysis, rather than transaction data, and by combining multiple checks to perform a single transaction that would list the originating financial institution as the payor.

³ The Mexican finance ministry, Secretaría de Hacienda y Crédito Público de México, responded with extreme restrictions on the amount of U.S. Dollars that Mexican financial institutions can process for their customers. For many individual Mexican customers, Mexican financial institutions could no longer accept more than \$4,000 in U.S. Dollars in a given month.

Wachovia and Wells Fargo's relationships with other financial institutions to the extent that Wells Fargo was processing transactions on their behalf.

I also spent several years as a Litigation Consultant with TM Financial Forensics, a consulting firm in San Francisco, where I assisted in consulting engagements on disputes stemming from processing, agency, custodial and other relationships between major financial institutions. Specific failures by those institutions related to oversight and verification of their relationships with other institutions have resulted in ongoing losses in excess of \$10 billion.

I have presented on the topics of financial and computer forensics, human trafficking, and organized crime for the Association of Certified Anti-Money Laundering Specialists, the California Narcotic Officers' Association, and the Southwest Border Anti-Money Laundering Alliance.

I was asked to provide the committee with an assessment as to how financial institutions monitor, review and verify depository relations with payment processors. I would like to begin by identifying the scope of these relationships.

Financial institutions may directly facilitate outside payment processing through several channels, including:

- Engaging a third party to process payment card transactions.
- Engaging a third party to process Automated Clearing House ("ACH") transactions.
- Maintaining accounts for money service businesses that facilitate payment card transactions, ACH transactions, wire transfers, e-checks, or remote deposits.
- Maintaining accounts for money service businesses that facilitate alternative payments, such as gift card redemptions or cryptocurrency.

Financial institutions may indirectly facilitate outside payment processing by associating with other financial institutions that are engaged in these activities.

Evaluation Types

Evaluation of payment processor activity by financial institutions is usually siloed by group depending on the purpose of the evaluation. The silo also informs the standard the financial institution uses to evaluate the payment processor.

- **Underwriting/Risk Assessment**
 - The standard for this type of evaluation is "a credible challenge." Underwriting/risk assessment teams prepare an evaluation that is sufficient to respond to a credible challenge of a payment processor's suitability for the financial institution.
 - This type of evaluation is performed as part of the ordinary management of the relationship between a financial institution and a payment processor. Members of a financial institution's business development team will assist the underwriting/risk management team in obtaining information about a payment processor's background, principals, creditworthiness, customer base, and expected transaction volumes.

- In some cases, such as with payment processors operating in high-risk jurisdictions or that maintain a high-risk customer base, additional scrutiny is applied to the potential relationship in a process referred to as Enhanced Due Diligence (“EDD”).
- EDD may include in-person interviews, on-site audits, extensive historical transaction data reviews, deep investigation of principal backgrounds, or other procedures that may not have been applied during the standard underwriting process.
- These evaluations are reviewed periodically and updated with new information based on actual transaction activity and updates provided by payment processors.
- **Fraud Investigation**
 - The standard for this type of evaluation is “potential loss.” Fraud investigation teams evaluate a payment processor relationship and determine whether the relationship will result in a potential loss to the financial institution.
 - Initial investigations are focused on transaction participants rather than their payment processors.
 - After a financial institution determines that a payment processor has been identified with significant losses to the financial institution, an investigation may be opened on the processor itself. This kind of escalation is exceedingly rare, in large part due to the work of the underwriting/risk management investigators. Losses would need to rapidly increase in a short period of time to route the evaluation of a payment processor to a fraud investigation team rather than the risk management team.
- **Financial Crime**
 - The standard for beginning this kind of investigation is identification of “unusual activity.” The standard for making a negative finding is identification of sufficient “suspicious activity.” Financial crime investigation teams evaluate payment processor relationships and determine whether the relationship has been compromised by money laundering or terrorist financing activity.
 - Much like fraud investigations, initial financial crime investigations are focused on transaction participants.
 - After a financial institution determines that a payment processing relationship has deteriorated such that a payment processor’s assertions regarding transactions are no longer reliable, an investigation may be opened on the payment processor itself. This kind of escalation is also exceedingly rare. However, unlike fraud investigations, these escalations are rare because money laundering does not typically result in a loss to the financial institution, even after payment of sanctions, fines, or penalties.
 - Jerry Robinette, a former Homeland Security Investigations Agent and bank compliance officer put it best, “*Until you start sending people to jail, the pockets are there to satisfy penalties...*”

Payments to Websites Facilitating Commercial Sex

To support an assessment of financial institution relationships with payment processors, I reviewed currently available payment options on four websites associated with the commercial sex trade: Humaniplex, The Erotic Review, Nightshift, and Rubmaps.

- Humaniplex is a classifieds site that allows users to purchase “FXPoints” to access most of the website’s features. Although there are ad sections related to employment, goods, housing, and personals, substantially all of the advertisements listed are in the escorting sub-section.
- The Erotic Review provides a platform for users of commercial sex to describe their experiences in great detail, including measurements, specific acts, and ambiance. Access to detailed descriptions of sex acts is limited to paid users.
- Rubmaps⁴ is a review platform specializing in “erotic massage parlors.” Access to most descriptions on Rubmaps is limited to paid users.
- Nightshift is a combined classifieds and review platform. Unlike Rubmaps and The Erotic Review, advertisers contribute much of the information related to the individuals being advertised. Early access to reviews, enhanced classifieds, and other benefits are limited to paid users.

Nightshift, Humaniplex, and The Erotic Review⁵ accept payments through CCBill, LLC⁶, a payment processor based in Tempe, Arizona. CCBill has had a payment processing relationship with Merrick Bank, based in South Jordan, Utah, for over a decade.

The Erotic Review offers a second credit card payment option through Rocketpay, a service provided by Rocketgate PR, LLC,⁷ a payment processor⁸ based in Puerto Rico.

Nightshift and The Erotic Review also accept cryptocurrency. Nightshift accepts multiple cryptocurrencies through Coinpayment, a cryptocurrency processor based in Vancouver, Canada.⁹ The Erotic Review limits cryptocurrency payments to Bitcoin and accepts payments through Bitpay, a cryptocurrency processor based in Atlanta, Georgia.

⁴ Rubmaps is also associated with Aaampmaps, an “Asian erotic massage” review site, Rubads, an escort classifieds site, and Eroticmonkey, an escort review site. Rubmaps appears to be the only site that currently accepts payments.

⁵ Nightshift and Humaniplex only accept payment cards. The Erotic Review accepts payment cards and ACH-based transactions.

⁶ CCBill was founded by Ira Ron Cadwell, a chiropractor, and currently processes over a billion dollars in online transactions per year. CCBill is widely used in the adult online entertainment industry and was described by The Independent as “the PayPal of porn and go-to online billing company for porn sites.”

⁷ Rocketgate PR, LLC is the successor to Rocketgate, LLC, originally formed in Las Vegas, Nevada by Jason A. Burns, a software engineer, and D’arcy Tyrell, a former NASA engineer.

⁸ Here, I refer to payment processors generically. Rocketgate provides payment gateway services, which process payments for one or more merchant accounts opened through a financial institution or their sales agents.

⁹ Coinpayment was founded in Atlanta, Georgia by Pawel Chrostowski and others. After FinCEN identified them as a money service business, the company was moved to Canada through a series of over the counter stock transactions.

Both Coinpayment and Bitpay offer their merchants the option of converting customer cryptocurrency payments to fiat currency. Bitpay settles U.S. Dollar transactions through ACH transfers sponsored by at least one U.S. financial institution, although Bitpay's CTO has publicly stated that those financial institutions requested that they not be named publicly.¹⁰

Coinpayment settles U.S. Dollar transactions through Coinbase, a cryptocurrency processor located in San Francisco, California. Coinbase facilitates these conversions using ACH transfers sponsored by Silicon Valley Bank in Santa Clara, California.

The Erotic Review also accepts payments through store-branded gift cards intended to be used at a single merchant through Paygarden, a gift card processor based in San Francisco, California. Paygarden publicly states that they are "integrated with USA gift card networks" and that they use those networks to "do real-time balance lookups and to reclaim the value on popular gift cards."

In other words, just as Safeway is able to load value onto a Starbucks gift card by virtue of its access to these gift card networks, Paygarden is able to extract value from those same Starbucks gift cards using its own access. Cashstar, currently owned by Blackhawk Networks, appears to be one of the networks being used by Paygarden. Cashstar's terms of service state the following,

"Gift Cards cannot be reloaded, resold, or transferred for value. Void if reloaded, resold, or transferred for value. Unused Gift Cards may not be transferred... Gift Card is not redeemable for cash"

Paygarden's terms of service appear to conflict with Cashstar's terms,

"Redeeming Gift Cards...Once you confirm a sale of a Gift Card to PayGarden, you agree to transfer ownership of the Gift Card and any interest therein to PayGarden"

Blackhawk Networks, Cashstar's parent company, has relationships with multiple financial institutions that are ultimately responsible for these transactions.

Rubmaps accepts credit card payments through Euro Payment Group GMBH nka EPG Financial Limited, a German payment processor. The transaction appears to take place entirely outside of the United States.

Money Laundering Red Flags

- Nightshift appears to be using a Cypriot shell company to accept credit cards through CCBill.
 - Nightshift's billing page states that "CCBill LLC is a designated payment processor for Himoto Limited."
 - Himoto Limited was formed in Cyprus and lists its sole shareholder as Altus Services Limited.
 - Altus Service Limited is owned by the Cypriot law firm, Chr. P. Mitsides & CO LLC. This law firm does not appear to be the ultimate beneficial owner of Nightshift.

¹⁰ Newsmax Finance, December 6, 2013, "Bankers Balking at Bitcoin in US as Real-World Obstacles Mount". "[Stephen Pair, co-founder and chief technical officer of BitPay Inc.] said BitPay has relationships with banks in the U.S., Canada and Europe; he declined to name them at the banks' request."

- The Erotic Review appears to be using a Cypriot shell company to accept credit cards through CCBill and Rocketgate.
 - The Erotic Review’s Terms of Service state that,

“Subscriptions to TER will be processed by THP Internet Resources or by such Third Party credit card processors (Such as CCBill or SegPay) with which THP Internet Resources may contract.”
 - THP Internet Resources Ltd.’s latest annual report indicates that Treehouse Park, S.A.¹¹, based in Anguilla, is a related party, and that THP Internet Resources Ltd. owed several hundred thousand euros to Treehouse Park, S.A. Substantially all funds received by T.H.P Internet Resources Ltd. are passed through to Treehouse Park, S.A.
 - The CCBill payment page states that CCBill is the payment processor for Treehouse Park, B.V., the Dutch subsidiary of Treehouse Park, S.A.
 - The Rocketgate payment page states that Rocketpay is the payment processor for T.H.P Internet Resources Ltd.
 - T.H.P Internet Resources Ltd. was formed in Cyprus and lists its sole shareholder as Richard Reideman, a Dutch national residing in Cyprus.
 - Treehouse Park, S.A. is wholly owned by another Anguilla entity, The Sycamore Trust, which is controlled by individuals other than Richard Reideman.
 - Reideman does not appear to be the ultimate beneficial owner of T.H.P Internet Resources Ltd.
- Rubmaps appears to be using a Cypriot shell company to accept credit cards through a foreign payment processor.
 - The Rubmaps logo on the billing page is a map of the United States with a white hand over it and the slogan “Find Your Happy Ending!”
 - Rubmaps’ billing page states that transactions will appear as “Miracomm R-Maps +18882246844.” “888” numbers are only toll-free in North America.
 - Miracomm is identified in Rubmaps’ terms of service as Miracomm Holdings Ltd in Cyprus. Miracomm Holdings Ltd currently lists Georgios Veniaminidis, a 74-year old resident of Cyprus, as its sole shareholder.
 - Miracomm Holdings Ltd was formed by CDP Media AG, a Swiss entity controlled by individuals other than Veniaminidis.
 - Veniaminidis does not appear to be the ultimate beneficial owner of Miracomm Holdings Ltd.
- Humaniplex allows users to transfer “FXPoints” to other users, effectively creating its own internal currency that is being used to pay advertisers for access to individuals being advertised on the site.

¹¹ Treehouse Park is a reference to an upscale part of Amsterdam in the Netherlands and the former location of The Erotic Review’s physical operations.

- One user stated bluntly, “... anyone sending me a [private message] from here are on must transfer me 40 fx points before I will ever respond to you”
- A photo-sharing “club” on the site has several requirements for admission, including a “One time fee of 580 FX points transferred to [the club owner] for use as prizes to the ladies that post.”
- Coinpayment moved its operations to Canada and publicly stated that this was done in order to evade FinCEN money service business requirements.
 - Coinbase and Silicon Valley Bank appear to be allowing Coinpayment to settle U.S. Dollar transactions.
- Paygarden’s business model does not appear to be consistent with the expectations of financial institutions participating in Blackhawk Networks’ gift card network. Paygarden specifically identifies Target and Bestbuy as sources of gift cards to facilitate anonymous payments. Target’s gift card purchasing site indicates that use of these gift cards to anonymously purchase subscriptions to The Erotic Review is inconsistent with Target’s expectations,

“Target GiftCards are solely for use at Target stores and on Target.com. If someone claims that you should pay them in Target GiftCards, please report it at ftccomplaintassistant.gov.”

Financial Institutions Cannot Replace Law Enforcement

Financial institutions have an excellent grasp on fraud prevention, detection, and mitigation. The threat of a potential loss justifies the resources required to address fraud effectively. The threat also creates a clear performance indicator – higher losses are bad, lower losses are good.

This is not the case with money laundering, and consequently not the case with payments processed for human trafficking rings and other criminal organizations. There is no clear benefit to the institution other than the vague idea that they’ve avoided reputational risk and trivial sanctions and penalties.

As we saw earlier, an examination of just four websites reveals that payment processors are extremely vulnerable to money laundering risks, and that those risks are not readily apparent to their sponsoring financial institutions. Those same financial institutions have limited incentives to invest in additional anti-money laundering infrastructure. I often hear the complaint from these institutions that they do not wish to take the place of law enforcement and that they feel regulators are increasingly requiring financial institutions to fill that role.

I do not dispute the need for someone to fill that role, but I believe that should be law enforcement rather than bank investigators. At some point, we have to realize that, years after the Bank Secrecy Act was implemented, we are still discovering billions of dollars being laundered through U.S. financial institutions.

A colleague of mine coined the term “subpoena surface area,” referring to all the potential exposure that a particular suspect or organization has to third party data collection. An effective understanding of an individual’s or an organization’s subpoena surface area can mean the difference between dropping a case and being able to advance a case by identifying, obtaining,

and analyzing data from any of hundreds of server farms, transaction processing systems, marketing databases, security systems, third-party software and service providers, intermediaries involved in creating or maintaining any of these, and other sources that remain untouched, even by intelligence agencies.

I would ask the committee to consider the following: the most consistent request for assistance that I have received from law enforcement at any level has been a request to identify what data is available at an institution and where it is available. The only reason I am able to provide that information is because I was previously a bank investigator.

Rather than ratchet up the pressure on financial institutions to capture more and more instances of money laundering or human trafficking, I would request that we take our next cue from a relatively recent California state law, SB 272.

This law requires local agencies to create catalogs of enterprise systems describing the data collected, application used to collect the data, the vendor, the system's purpose, the department responsible, and the frequency that the data is updated.

A database of catalogs describing these kinds of systems at financial institutions would provide the information on subpoena surface area necessary to conduct complex money laundering investigations, it would protect consumer privacy by allowing law enforcement to narrowly craft subpoenas and search warrants, and it would reduce inordinate pressure on financial institutions to police their own customers beyond what current law requires.

Thank you again for this opportunity. I would be happy to answer any questions.