Business Case Study:
Largest U.S. Savings & Loan sees 80-to-1 R.O.I.
from Ultra-Violet Project

Executive Summary

Financial institution fraud losses have been steadily rising during the last 15 years. The advent of digital graphics, printing and home-publishing technologies has armed criminals with the tools needed to enact a broad array of counterfeit theft activities against banks and other financial service organizations. The U.S. Dept. of Treasury's Financial Crimes Enforcement Network (FinCEN) has tracked fraudulent behaviors in the financial services industry since 1994, and their data shows rapid yearly increases in the number of fraudulent cases involving counterfeit documents.

Washington Mutual Bank (now a part of J.P. Morgan Chase) has installed more than 29,000 pieces of UVeritech's Fraud Fighter™ *ultra-violet* counterfeit detection devices into its retail branch locations. The final purchase of nearly 22,000 pieces, in July 2007, was the culmination of a carefully planned and monitored field-trial of the products which proved the concept of using UV lights as an effective fraud-prevention method for the branch-banking marketplace, capable of producing unprecedented Return-on-Investment.

Ultra-Violet lights are a flexible and effective tool which can be used to validate the authenticity of a majority of the important documents presented by customers to bank employees at bank branch locations. Simple to use, and remarkably easy to integrate into any business operation, the Fraud Fighter™ UV devices purchased by WAMU enabled tellers, loan officers, new accounts representatives and branch managers to validate currency, driver licenses, passports, credit cards, social security cards, and a variety of other negotiable instruments and identity documents.

The Strategic Sourcing division of WAMU determined after the initial pilot project was conducted that annualized savings produced through the prevention of fraudulent loans and other counterfeit document losses was greater than $20,000,000, even though only 1/3 of the branch network was provided with the equipment. The cost to equip the first 800 branches with the equipment was only $225,000. Thus, ROI on the pilot project was greater than 80-to-1 during the first year of use. Based on these numbers, the decision was made to roll-out to entire branch network.

Washington Mutual

WAMU was the largest savings and loan association in the United States before it was forced into receivership by the FDIC due to its non-performing loan portfolio. In 2008, prior to the acquisition by JPMorgan Chase Bank, Washington Mutual Bank had total assets of US$307 billion, with 2,239 retail branch offices operating in 15 states, 4,932 ATMs, and 43,198 employees[1].

WAMU pioneered certain practices which were considered revolutionary within the industry. One of these was the casual design of bank branches, which did away with the old-fashioned teller-line and placed tellers at kiosks. In 2003, then CEO Kerry Killinger put WAMU on the course of dominating the sub-prime lending business, building WAMU into the "Wal-Mart of Banking," which would cater to lower- and middle-class consumers that other banks deemed too risky. Complex mortgages and credit cards had terms that made it easy for the least creditworthy borrowers to get financing, a strategy the bank extended in big cities, including Chicago, New York and Los Angeles.

As a result of their aggressive activities in the marketplace, the total number of WAMU customers grew exponentially, and the "customers per branch" service ratio was the highest in the industry.

WAMU Bank Branch Fraud

Every aspect of WAMU's retail bank operations was exposed to counterfeit fraud. Criminals used false I.D. documents with stolen identities to open money–laundering bank accounts, and to fraudulently apply for credit. At the teller window, WAMU was unprotected against losses resulting from counterfeit money and fraudulent checks. With the recent advent of advanced digital scanning and printing equipment, this exposure was greatly amplified. By 2005, just about any person with a PC, a printer and fundamental digital graphics skills was able to produce highly accurate counterfeits of most of the items being presented at the bank branch.

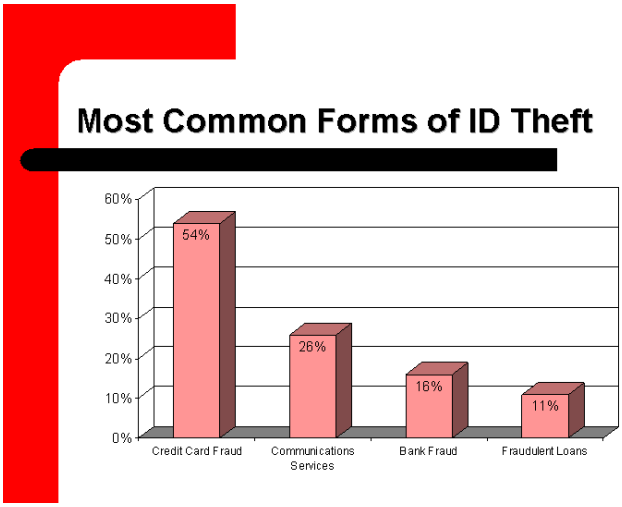
By 2007, these technical advances and the globalization of counterfeit fraud rings were providing increasing operational challenges for WAMU. In the bank branch, each location in the branch which served as a point of contact with the public was a potential "breach". Teller window, new account desk, loan desk, investments and retirement

[1] "OTS Fact Sheet on Washington Mutual Bank" (PDF). Office of Thrift Supervision. 2008-09-25. http://files.ots.treas.gov/730021.pdf. Retrieved 2008-09-28.

planning, safety deposit counter. Each had its unique set of regulatory obligations and potential fraud exposures.

Due to the varied transactions conducted in their service centers, WAMU found that they were exposed to a complex range of fraud, and that they had no comprehensive process or tool to apply towards the problem. Losses at the branch level were occurring throughout the entire range of services provided at the branch location.

Counterfeit negotiable instruments were frequently passed into the WAMU branches, with the bank not realizing the loss has occurred until well after the fraudulent transaction had passed. Counterfeit currency had been a growing problem for more than a decade, but even more worrisome were phony Postal Money orders, cashier's checks, traveler checks and payroll checks, which were difficult to scrutinize due to the number and variety of different issuers of these instruments.



Through the use of false or stolen identification, criminals were accessing deposit accounts that were not theirs, applying for credit against existing customer accounts, setting-up fraudulent HELOC loans, laundering money through investment accounts and by wire transfers, and taking cash advances against stolen credit cards.

By far, WAMU's greatest exposure lay in the credit-issuance portion of the operations. While counterfeit currency and negotiable instrument fraud losses may have totaled "thousands of dollars" per branch on an annual basis, the issuance of fraudulent credit was responsible for "tens of thousands" of dollars per branch. Intelligent fraud rings were learning the thresholds for loan amounts that did not trigger advanced scrutiny, and would target branches systematically, producing false identity documents to replicate current WAMU customers and applying for HELOC's for less-than $100,000, and for credit-cards with limits of typically less than $5,000.

Although Fraud Fighter™ was never formally notified of total fraud losses experienced by WAMU, the problem seems to have been very significant – ranging to as high as $50M or more annually.

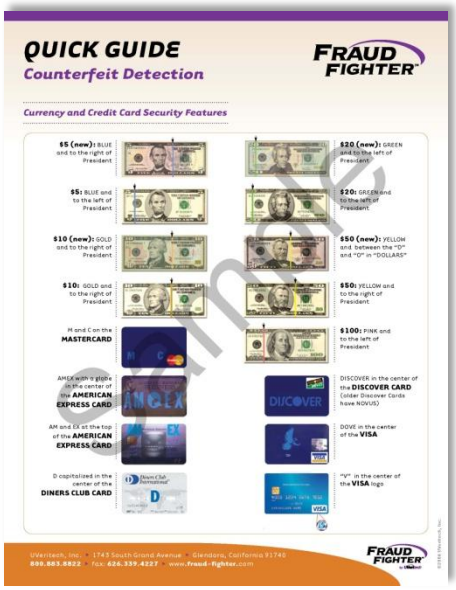
UVeritech as Fraud Prevention Partner

UVeritech, founded in 2000, began its business by providing *ultra-violet* counterfeit detection solutions to the financial services industry. In 2001, Wells Fargo became the first "national" customer to integrate UV lights into their branch operations. This was followed in 2002 by Bank of America. By 2007, when WAMU had completed their pilot

project, these two national bank operations had already installed more than 40,000 Fraud Fighter™ UV lights into their branch locations. Additional Fortune 500 financial service customers that had conducted system-wide installations to their branch networks by this time included Regions Bank, Union Planters, Citizens Bank, Bank of the West, and many others. The Fraud Fighter™ line of UV products was endorsed by nearly half of the state banking associations in the country, and the products were in-use by over 1,500 bank and credit union customers.

The explanation for this widespread adoption of Fraud Fighter™ products by the banking industry is not difficult to understand. *Ultra-Violet* lights offer the bank branch a remarkably flexible tool which can be used to authenticate currency notes, driver licenses, passports, social security cards, traveler checks, money orders, credit cards, and a wide variety of other important documents. The integration of the UV lights into the bank branch is simple – with no network or internet connections, no software installations or updates, and very little product training required, the installation in the branch was typically performed by the branch-level employees. The Fraud Fighter simply needs to be removed from its box, plugged-in and turned on.

In addition to flexibility and ease of use, the cost of ownership of Fraud Fighters is so low, that many potential buyers of the product think there must be some hidden costs involved. Under the correct circumstances (e.g. – an enterprise roll-out), the cost to equip a branch location, which might involve the purchase of as many as 10 units to cover teller, new account and loan desk areas, will be less than $500. The Fraud Fighters carry a lifetime warranty, so the true cost of ownership <u>is</u> the initial purchase price for the machine.



UVeritech has enhanced the usefulness of our Fraud Fighter™ *ultra-violet* detectors in the branch by developing detailed training materials which enable the branch-level employee to quickly and easily learn how to use the equipment and what security features to look for in the various documents they may be looking to verify. These "Quick Guides" provide detailed 4-color images showing the teller how genuine items should appear when reviewing the document under the *ultra-violet* illumination.

For some customers with specific applications for which they want their employees to utilize the Fraud Fighters, UVeritech develops customized training materials, pulling information and images from our extensive library of images and data. One such example is the identity verification guide pictured to the left.

In most cases, the simplicity of using the UV lights is such that cashiers and tellers are able to learn the information within minutes and do not require access to training materials on a regular, ongoing basis. However, UVeritech does continue to provide updates whenever changes occur to these official documents (for example, a banknote redesign or new driver license template), so the employees are constantly re-exposed to the informaiton when these updates are released.

WAMU & UVeritech – A Partnership for Success

Rather unusually, the relationship between UVeritech and WAMU began as the result of an ambitious and energetic branch manager in Orange County, CA whose branch was suffering from identity related fraud. After seeing a demonstration of the UV-16 product in his branch, the manager bought 8 units with his personal credit card. This was in November of 2004.

Under normal circumstances, UVeritech tries to develop enterprise relationships with corporate managers involved in asset protection or loss prevention. In typical solution-selling style, UVeritech has always sought to achieve Sr.-level "buy-in" to the concept of Fraud Fighter™ solutions before any in-store testing is conducted. WAMU proved that the opposite model can also work, and that "store level" employees can be the catalyst for change.

Tales of this O.C. store's results began spreading via the grassroots network of employees and branch managers. Apparently, an epidemic of false identity related fraud was striking WAMU branches throughout the Southwest. Such fraud events ranged from cashing stolen checks and taking cash advances against stolen credit cards to applying for HELOC loans against WAMU customers' properties. In common with these fraud losses was the use of false identity documents which matched the information of the targeted accounts.

As word spread, UVeritech began fielding a steady flow of inquiries from branch managers who had heard about the equipment. In this way, through the first several months of 2005, UVeritech equipped roughly 50 branches with the UV-16 product – almost entirely purchased by store managers on personal credit cards.

By the Spring of `05, the attention of the SoCal regional asset protection manager had been gained, and discussions advanced rapidly to the point where UVeritech had been invited to present to the regional WAMU HQ located in Northridge, CA. There, the Vice President and Sr. Manager of Corporate Security and his team responsible for managing security for WAMU's entire branch network discussed the fraud issues they were suffering and their plans to address them. The success seen with the use of the Fraud Fighters in the early-adaptor branches had sufficiently impressed this team of asset protection managers to fast-track the testing of the equipment into a more widespread pilot project. The initial targeted pilot would look to place units into 70 branch locations in California and Florida. 800 units were shipped to "problem" branch locations in June, 2005.

Less than 90 days later, the project manager reported that "the pilot project had been very successful". Pressed for details, it was revealed that a fraudulent home loan had been prevented during the first week, dozens of stolen/false checks had been caught throughout the test period, and numerous incidences of false currency had been prevented. In the case involving a fraudulent loan application, the criminal was in the branch and picking-up the cashier's check for a $92,000 HELOC, when the branch manager decided "on a whim" to test the ID document with the newly arrived Fraud Fighter™ UV-16. As a result of discovering the false ID document, the perpetrator and two accomplices waiting in the parking lot were arrested.

Based on this monitored pilot project, it was decided that WAMU would be equipping branches with the Fraud Fighter™ UV lights on a more widespread basis. Control of the project was shifted to the national HQ in Seattle, where a new project management team was assigned.

At this point, WAMU management was looking for the appropriate techniques and processes to ensure success for the roll-out of the products. Of particular concern were two primary matters: First, how to physically integrate the equipment into the branches, which were involved in redesign projects to move to the "Occasio" branch design featuring kiosks instead of teller windows. Second, how to ensure that branch employees were properly informed of how to utilize the equipment.

For both these issues, FraudFighter™ partnered with the WAMU project team to respond with solutions to the issues. In the case of the first issue – physical integration - UVeritech chose to re-engineer the two products chosen by WAMU in order to fit the physical space limitations of their new branch designs. Faced with height and width restrictions in the kiosk locations where the equipment was to be installed, UVeritech redesigned both the UV-16 and POS-15 products to fit the available space. Thus, the current product designs, which minimize the "footprint" needed, is the result of WAMU's need to fit the units into their workstations.

Re-Designed UV-16

The training issue also involved the development of customized training materials so that each unit came equipped with a booklet and several "quick guides" which enabled both ease of training and made available ongoing reference materials for the branch employees. As with the changes to the physical design of the units, the changes to the training materials were also incorporated into the Fraud Fighter™ standard package and all of our customers now receive this as a free benefit.

On July 31, 2007, WAMU issued a PO for the purchase of 21,780 additional units. This purchase was a combination of POS15 units and UV-16 units. The total cost of this PO, including shipping, taxes, etc., was less than $800,000. In total, WAMU has purchased approximately 29,000 pieces of UVeritech UV-based Fraud Fighters. The total investment in this equipment has been approximately $1.3 MM.

We are aware ONLY of the savings generated during the first widespread trial of the unit begun in January of 2006 This limited roll-out to less than 40% of branch locations produced savings of more than 18 times the cost of ALL UNITS PURCHASED to equip the entire national branch network. Assuming that ongoing savings in 2007, 2008, 2009 and 2010 have been more significant, due to the much wider roll-out to the national branch network, it is not difficult to extrapolate total return on investment over a 5 year period for the Fraud Fighter™ equipment could reach greater than 200 dollars for every dollar invested.

Summary and Conclusion

Regardless of the information source, whether it be FinCEN, Lexis-Nexis, the American Association of Certified Fraud Examiners, or the American Banker's Association, it is obvious that the general trend over the past decade has been a steady increase in the dollar losses suffered as the result of fraud by financial institutions.

Washington Mutual saw this trend and was able to conduct a systematic analysis to determine whether the grass roots movement cultivated through the actions of a single branch manager could be translated to, first, a regional, and next, a national roll-out of *ultra-violet* lights into their bank branches.

The results proved to be nothing less than extraordinary. After conducting a large sample roll-out of product into 800 branches, WAMU experienced a return-on-their-investment of greater than 80 dollars for every dollar spent. This happened during the first year of use. Presumably, similar fraud losses were prevented in the years since then.

Based on this result, WAMU management easily made the decision to continue the roll-out to their entire branch network – an additional 1400 branches.

With BofA, Wells Fargo, Citizens, Regions and WAMU all using the equipment on a national basis, it can clearly be stated that the use of *ultra-violet* lights in bank branch locations has become generally accepted as a best-practice for fraud and compliance related issues involving document verification during financial transactions.