Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

Fringe Financial Product Privacy and Security White Paper

Consumer Federation of America

Jean Ann Fox

September 2009

Table of Contents

Introduction

Sensitive consumer personal and financial information is collected by financial service providers ranging from heavily-regulated depository institutions to store-front fee-based alternative financial retail outlets. Personally identifiable financial information held by companies with lax or nonexistent privacy and security protections can expose consumers to invasions of privacy, as well as to identity theft and targeted marketing without real consumer consent.

Federal regulatory and state law enforcement cases have mostly targeted large financial institutions, such as banks and credit card issuers that mishandle personally-identifiable transaction information. For example, actions by state Attorneys General and private litigation have sought to stop credit card issuers from providing customer transaction information to third parties that market extra products. Following public disclosures of security breaches at large database companies, retailers and others, federal and state legislators adopted security freeze laws to protect consumers.

Less attention has been paid to informational privacy and security risks related to the practices of fringe financial service providers such as check cashers, payday loan outlets and websites, tax return preparers, and other high cost credit providers that serve a mostly low to moderate income clientele. These providers, although subject to the same federal financial privacy requirements as banks, are lightly regulated by an under-resourced Federal Trade Commission and a patchwork of state regulators whose priority is compliance with state licensing requirements. These companies collect sensitive consumer information in loan applications, such as Social Security numbers, bank account numbers, and transaction data. Some high cost financial products are particularly risky because providers hold extensive private financial information about borrowers.

The subprime sector includes check cashers, payday lenders, car title loan outlets, small installment lenders, tax preparers who sell refund anticipation loans, and providers of prepaid cards to consumers who do not have bank accounts. Consumers weigh many factors in choosing to buy these products, but evaluating privacy and security risks is difficult and often impossible. Consumers in the sub-prime financial services market have little clout to refuse services that fail to protect privacy. While these companies are subject to the Gramm-Leach-Bliley Act and to Federal Trade Commission security rules, consumer privacy and security is not guaranteed. And, as the Texas Attorney General noted in a case against a high cost lender, a written privacy and security policy is no guarantee that the store will safeguard sensitive consumer information.

This White Paper is accompanied by a review of the laws that apply to non-bank financial service providers and by information on how to contact state and federal regulators. The White Paper provides an overview of privacy and security policies and practices for fringe financial services and explores in more depth the unique design features of two high cost credit products that elevate concerns about consumer safety. The CFA Handbook on Federal and State Legal Protections of Consumers' Financial Information Privacy and Security describes in detail the federal and state laws that govern the handling of personal financial information by the non-bank sector. [1] CFA also provides a directory of state Attorneys General and Credit Regulators who are

[1] CFA Handbook: Federal and State Legal Protections of Consumers' Financial Information Privacy and Security, September 2009.

responsible for enforcing state rules on identity theft, financial privacy and security, and for regulating nonbank financial providers, as well as contact information for federal Financial Regulators and the Federal Trade Commission. CFA also has prepared a directory of state Insurance Regulators who are responsible for supervising insurance companies' compliance with privacy and security requirements.[2]

Privacy and Security Risks at Fringe Financial Providers

The potential risks to consumer privacy and security when doing business with non-bank financial service providers can include theft or misuse of personally identifiable financial information, lax handling of consumer financial documents, sharing personal information with third-parties, and tracking of consumers' online browsing history.

ID Theft

Identity theft happens when a person uses the victim's personal identifying information without permission to commit fraud or other crimes. This information includes name, Social Security number, credit card or bank account information. Once a thief has stolen bank account information, for example, he can create counterfeit checks using the victim's name or account number; open a bank account in the victim's name; clone an ATM or debit card to make electronic withdrawals; or take out a loan in the victim's name. An identity thief may file a fraudulent tax return and obtain a tax-related loan, using the victim's information.[3]

The Federal Trade Commission's Consumer Fraud and Identity Theft Complaint Data for 2007 noted that identity theft was the number one consumer complaint category for the eighth year in a row. Of 813,899 total complaints received in 2007, thirty-two percent (258,427) were related to identity theft.[4]

The same pattern of complaints was reported by the FTC's Consumer Sentinel Network Data Book for 2008. Identity theft was the top complaint category for complaints filed through the inter-agency Consumer Sentinel Network, accounting for twenty-six percent of all complaints. Within the ID theft category, credit card fraud was the most common form reported, followed by government documents or benefits fraud, employment fraud, and phone or utilities fraud. The FTC reports that fraudulent tax return-related identity theft has increased nearly six percentage points since calendar year 2006. Electronic fund transfer-related identity theft was the most often reported type of identity theft bank fraud in 2008, although the number of complaints has declined since 2006.[5]

---

[2] The White Paper author is Jean Ann Fox, Director of Financial Services, Consumer Federation of America (CFA). Paul Stephens, Privacy Rights Clearinghouse, contributed an evaluation of privacy and security policies used in writing the White Paper. Mark Silbergeld, CFA Senior Fellow, wrote the Handbook. Darby Hull, CFA Legislative Assistant, compiled the state resource directory. This White Paper is supported by cy pres funding but its content is the responsibility of CFA.

[3] FTC "About Identity Theft – Deter. Detect. Defend. Avoid ID Theft," http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html, viewed September 19, 2008.

[4] FTC Press Release, February 13, 2008, reproduced at http://www.ftc.gov/opa/2008/02/fraud.shtm, viewed May 21, 2009.

[5] FTC "Consumer Sentinel Network, Data Book for January-December 2008," February 2009, at 3. Reproduced at http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sectinel-cy2008.pdf, viewed May 22, 2009.

The Federal Trade Commission provides a handbook for consumers to help combat identity theft. The online document includes information on the many ways identity theft occurs such as stealing records or information from places of employment, taking mail (bank and credit card statements, credit card offers, new checks, and tax information), "dumpster diving" or rummaging through the trash of a business; and stealing credit or debit card numbers by capturing the information via a data storage device.[6]

The Federal Trade Commission commissioned an ID theft survey of US adults in 2006 to learn about the prevalence of victimization, the impact on victims, actions taken by victims as well as ways to help victims of future cases of ID theft. Approximately 8.3 million U. S. adults found themselves victims of some form of ID theft in 2005.[7] While over half of ID theft victims do not know how their information was stolen, 16 percent know their thief personally; five percent said the information came from a company, and seven percent of cases involved information stolen during a purchase or other transaction.[8] The FTC survey found that problems experienced by ID theft victims included debt collection harassment, the need to repeatedly correct credit records, problems getting credit, and banking problems.

A study by the Center for Identity Management and Information Protection at Utica College, which looked at more than 500 Secret Service criminal identity theft cases closed between January 2000 and March 2007, found that many cases involved sloppy data-security practices by retail businesses. Less often, ID theft resulted from thieves getting information from victims' friends, relatives or co-workers. The ID theft offenders described by the study were 54 percent black while 38 percent were white and nearly one third were women. Over 70 percent of offenders had no criminal record. About half the cases studied involved use of the Internet and most were interstate in nature.[9] The study found that in most cases, identity theft facilitated other offenses, most often fraud, followed by larceny. Organized groups of two to 45 people could be identified in over 40 percent of the cases. Victims of the ID theft cases studied by Utica College included financial institutions which were most frequently victimized by offenders using fraudulently obtained personal identifying information to get new credit cards, apply for and get fraudulent loans, to get checks cashed and to transfer funds.[10]

Other Risks to Consumer Privacy

In addition to identity theft, the risks to consumer privacy from fringe financial service providers include secondary use of information for targeted marketing, customer profiling and tracking, and adverse decisions based on inaccurate or incomplete information. For example, many sub-prime lenders and retailers only report negative information to credit reporting agencies. And, information shared among affiliate and third-party companies in the sub-prime sector help to keep consumers trapped in high-cost, high-risk products and services. Sensitive personal information, such as tax returns, is shared with banks to make loans secured by expected tax

---

[6] FTC, "Take Charge: Fighting Back Against Identity Theft," http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm, viewed January 7, 2009.
[7] FTC, "Federal Trade Commission 2006 Identity Theft Survey Report," November 2007 at 4.
[8] *Ibid*, at 20.
[9] Christopher Conkey, "Identity Thieves, Methods More Diverse Than Believed, Study Finds," *Wall Street Journal*, October 20-21, 2007 at A 5. See also, Press Release, "Center for Identity Management and Information Protection to Release Landmark Study," Utica College, October 17, 2007.
[10] *Ibid.*

refunds. Consumers of fringe financial outlets are at risk from unsafe handling and disposal of loan applications and other information held by providers.

Consumers who use the Internet to access high cost financial service products, such as payday loans, can also be tracked without their knowledge with information used to target loan offers. Online behavioral tracking and targeting can be used to take advantage of vulnerable consumers. Behavioral advertising is the practice of collecting and compiling data from and about an individual's activities, interests, preferences, behaviors or communications online for targeting advertising and marketing to that individual. Information about a consumer's health, financial condition, age, sexual orientation, and other personal attributes can be inferred from online tracking and used to target the person for payday loans, sub-prime mortgages, bogus health cures and other dubious products and services.[11]

Social Security Number Access and Fraud

Social Security numbers provide the key to unlock a consumer's financial identity. A poll conducted by the Consumer Reports National Research Center found that 89 percent of Americans want state and federal lawmakers to restrict the use and availability of Social Security numbers by businesses and government agencies. In the year prior to the 2007 poll, 87 percent of consumers had been asked to provide their Social Security number in whole or in part by a business or government agency. These numbers are used to identify and authenticate the identity of individuals. Consumer Reports found that 91 percent of respondents agreed they are more vulnerable to identity theft when a business has their Social Security number while 96 percent agreed that companies should not be able to sell these numbers.[12]

Privacy and Security Policies at Fringe Financial Outlets

Federal law requires all of the financial service outlets described in this paper to provide information to consumers on their rights regarding information collected from consumers, used by the provider, and shared with affiliates and third-party companies. The Gramm-Leach-Bliley Act (GLB) regulates the privacy and information security practices of both traditional and fringe financial providers.[13] Financial companies must provide a notice to consumers that describes the financial institution's policies and practices concerning the disclosure of present and former customers' nonpublic personal information (NPI) to affiliates and nonaffiliated parties, including the categories of information that may be disclosed. (See the Handbook for a full explanation of the Gramm-Leach-Bliley Act requirements).

Privacy policies must identify the categories of NPI that the institution collects, that it discloses, and the categories of affiliates and nonaffiliated third parties to whom the institution discloses NPI.[14] If NPI is disclosed to a third party that performs services for the institution, or markets products or services under joint marketing agreements, the institution must disclose the

[11] CFA, "Online Behavioral Tracking and Targeting Legislative Primer," September 2009, http://www.consumerfed.org/pdfs/OnlinePrivacyLegPrimerSEPT09.pdf.
[12] Consumers Union, "Consumers Union Calls for Limits on Social Security Number Use & Availability," December 11, 2007, available at http://www.consumersunion.org/pub/core_financial_services/005278.html, viewed January 7, 2009.
[13] 15 USC Sections 6801-6809
[14] 16 CFR 313.6(a) (1), (2), and (3).

categories of NPI that it discloses and the categories of third parties with whom the institution has contracts.[15] These companies must tell consumers about their right to opt out of disclosure of NPI to nonaffiliated third parties and the methods to use to opt out.

Under GLB, consumers generally have no right to opt out of having their information shared among affiliates of the same company. However, the Fair Credit Reporting Act gives the right to opt out of information sharing on "creditworthiness," but not "transaction and experience" data.[16] Financial companies also have to disclose their policies and practices for protecting the confidentiality and security of NPI.[17]

Privacy policies posted by companies as a result of these legal requirements may not be as informative as consumers expect, since providers are only required to include categories of information shared and a few illustrative examples of the type of NPI that may be collected or disclosed, not a complete list of everything a company collects or everyone who might see personal financial information.[18]

The information fringe financial outlets collect depends in part on the type of service being provided, with simple check cashing on one end and tax preparer-sold refund anticipation loans on the other. Typically financial service providers collect information given by the customer on applications or provided to obtain a product or account. Information is collected from third parties such as consumer reporting agencies and other nonaffiliated parties. And, companies collect information internally and from affiliates on transactions and experience in using their product or service.

Information collected directly from consumers on loan applications would typically include:

- Name, address, and phone numbers
- Social Security number
- Mother's maiden name
- Employment information
- Asset and income information
- Driver's license and other identifying information
- Birth date

Tax preparers selling financial products have the entire tax return and the supporting documents that taxpayers bring in for tax preparation purposes. Typical payday loan applications request the borrower's personal information, Social Security number, bank account and routing number, job references or copies of Social Security award letters. A typical car title loan application from Utah requested the usual customer identification information, employer contact information and payment schedule, vehicle year, make, model, tag, value and VIN number; reference names, addresses, phone numbers and relationship to loan applicant; and information on how the borrower heard about the lender. A rent-to-own application from the Salt Lake City area asks for identifying information including a Social Security number, vehicle make, model and license

[15] 16 CFR 313.13-14
[16] 16 CFR 313.6(a)(7)
[17] 16 CFR 313.6(a)(8)
[18] 16 CFR 313.6(c)

plate numbers and color of the vehicle; employer information including which shift the applicant worked; personal references, questions on whether the applicant had payday, car title loans or rentals from another company.[19]

Consumers who complete applications online also typically have the following information collected by the financial provider:

- IP address and internet service provider
- Browser type
- Cookies
- Web beacons
- Referring and exit pages

Some fringe financial institutions explain their information collection practices in a generic fashion, such as "information from applications and forms submitted by the consumer," "information about transactions and experience," and "information from affiliates and third parties (including credit reporting agencies)."

Financial companies are required under the Patriot Act's customer identification program (CIP) to collect customer Social Security numbers to prevent financing of terrorist operations and money laundering. CIP rules require that financial institutions collect name, birth date, and a physical address other than a post office box.

Fringe financial companies that disclose NPI must explain their policies. Typical language used to do that includes "we may use and share all of the information we collect," "we may disclose all of the NPI that we collect," we may disclose the information we collect in the paragraph titled "'information we collect,'" or "we may disclose NPI about you to affiliates and nonaffiliated third parties." (See Handbook Section IX on tax return privacy for more information on the restrictions placed by the Internal Revenue Code and IRS rules on disclosure of tax returns to sell financial products.)

Federal regulations prohibit a financial institution from disclosing "an account number or similar form of access number or access code for a consumer's credit card account, deposit account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer" with exceptions for disclosures to credit reporting agencies, service providers, and private label credit card programs.[20]

CFA reviewed a sample of privacy and security policies from a cross section of non-bank financial service providers to learn more about information sharing practices, ability of consumers to opt out of information sharing, and claims for secure handling of customer records. Below we describe typical privacy policy provisions with illustrative examples from these financial service companies.

Disclosure of NPI to Third Party Non-Affiliates

[19] Generic loan application for a car title loan and Action Rent-to-Own application, Utah, on file with author.
[20] 16 CFR 313.12

Since fringe financial service providers hold sensitive personal financial information, their policies for sharing this information with others are important for customers. They may share NPI with other financial companies, such as insurance or mortgage companies, and with non-financial entities, such as retailers, direct marketers, telemarketers, survey companies and organizations. For example:

- Cash America's online payday loan operation, CashNetUSA, provides a long list of companies with whom their customers' information may be shared: "The CashNetUSA Related Company delivering this Privacy Policy to you (the 'CashNet USA Provider") may share or sell Your Information with any other CashNetUSA Related Company (collectively, its "Affiliated Companies" and with other companies with whom any CashNetUSA Related Company does business ("Non-Affiliated Third Parties") as permitted by law and described in this Privacy Policy. These Affiliated Companies and Non-Affiliated Third Parties may be (1) financial service providers, such as mortgage bankers, mortgage brokers, consumer lenders, small loan lenders, tax refund anticipation loan lenders, loan brokers, deferred deposit providers, check cashers, supervised lenders, delayed deposit providers, deferred presentment providers, collection agencies, consumer reporting agencies, banks, credit card providers, debit card providers, store valued card providers, insurance agencies, bill payment agencies, ATM providers, pawn and title pawn providers, automobile dealers, automobile financing providers, automobile leasing providers, money transfer and remittance providers, sellers and remitters of money orders, insurance services providers, and financial service provider holding companies, or agents, contractors, or representatives of any of the foregoing; (2) non-financial companies, such as retailers, tax preparers, payroll service providers, advertisers, marketing companies, lead generators, advertisers on our websites, companies or individual that do industry-related research, surveys or polls, automobile dealers, and any person who offers a non-financial product or service, any holding companies, or agents, contractors, or representatives of any of the foregoing; and (3) other businesses, such as non-profit organizations, trade associations, and industry analysts or agents, contractors , or representatives of any of the foregoing.

  Affiliated Companies and Non-Affiliated Third Parties may use Your Information for any legal purpose, including, but not limited to, developing and promoting new or joint products, improving existing products and services, and contacting you to offer products and services that may be of interest to you. We may also disclose Your Information, as described above, to companies who perform services on our behalf or to other financial institutions with which we have joint marketing agreements."[21]

- The Urgent Money Service Family of Companies' policy on sharing information states in its privacy policy: "Unless you tell us not to, we may share with the Urgent Money Service family of companies certain information about you including: Information we obtain from your application or otherwise, such as your name, address, social security number, and income; Information we obtain from a consumer report, such as your credit history; Information we receive from your tax returns and associated documents including but not limited to payroll stubs, W-2 forms, W-4 forms, etc.; Information we obtain to verify representations made by you, such as your bank account information; and Information we obtain from a person regarding employment, credit, or other relationship with you, such as your employment history. The categories of companies who may receive this information are: Financial service providers, such as lenders, collection agencies, loan brokers, check cashers, post-dated check cashers, deferred deposit providers, deferred presentment providers, supervised lenders, delayed deposit providers, small lenders; and Others, such as any company that may offer a product or service that we believe would be useful, helpful and convenient to you such as tax preparers."[22]

Disclosure of NPI to Affiliates

[21] CashNetUSA ALERT, www.cashnetusa.com/privacy_policy.html, viewed 8/10/09.
[22] Urgent Money Service, Inc. Privacy Policy, http://www.urgentcashadvance.com/_policy.asp, viewed 8/11/09.

Financial services companies frequently share NPI with their affiliates. While consumers can opt out of their information on "credit worthiness" shared with affiliates, they have no control of the sharing of transaction and experience information with affiliates. Some companies disclose very generic information about their policies while others list the names of affiliates with whom they share information. For example:

- Valued Services, LLC states in its privacy policy: "We may disclose all of the information that we collect, as described above. We may disclose that information about you to the following types of third parties…. Companies affiliated with us by common ownership or control." On the second page of the privacy policy under "Your Choice to Limit Marketing From Our Affiliates (Opt-out), Valued Services spells out who these affiliates are. "You may limit our affiliates, including CompuCredit Corporation, Fortiva Financial Group, Inc., Credit Logistics, LLC, CAR Financial, the Valued Services Family of Companies, the Just Right Auto Sales Family of Companies, PML Wireless, LLC, and ACC Holding LLC from marketing their products or services to you based on your personal information that we collect and share with them. This information includes your income, your account history with us, and your credit score."[23]
- Advance America's privacy policy lists the categories of companies within the Advance America family of companies who may receive the information they collect: "Financial service providers, such as lenders, collection agencies, loan brokers, check cashers, post-dated check cashers, deferred deposit providers, deferred presentment providers, and delayed deposit providers; and Others, such as any company that may offer a product or serve that we believe would be useful, helpful and convenient to you."

Disclosure of NPI With No Opt Out Rights

GLB is full of exceptions that undermine consumer control over their nonpublic personal information. Typically NPI is shared with a financial entity's service provider for work such as preparing statements, printing checks, operating a call center, or processing transactions. Most troubling is the exception for financial institutions to share NPI for "joint marketing" purposes. Consumers have no right to opt out of information sharing when a financial entity enters into joint marketing agreements with telemarketers or direct mail marketers.[24] Most fringe financial providers take full advantage of this exception.

- Advance America "Service Provider/Joint Marketing Companies" notice: "We may disclose all of the information we collect, as described above, to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements, such as banks. Your right to opt out, as described below, does not apply to the disclosures described in this subsection, which are permitted by law."[25]
- Payday lender Check 'n Go's privacy policy section on "Information We May Share Even After You Opt Out:" "Your election to opt-out will not block our sharing of nonpublic personal information about you with nonaffiliated third parties that perform marketing services on our behalf or with financial institutions with whom we have a joint marketing agreement. This nonpublic personal information includes the following types of information about you: name, address, home and work phone numbers, e-mail address, social security number, time at residence, source and amount of income, and

[23] First American Cash Advance Privacy Policy Notice – Valued Services LLC, http://fa-ca.com/privacy.php, viewed 8/10/09.
[24] 16 CFR 313.13 exception of the Privacy Rule.
[25] Advance America Privacy Policy, obtained at www.advanceamerica.net (05274_00/0102/00622137.DOC2).

payment history. Additionally, your election to opt-out will not prevent us from disclosing to our affiliates the information we obtain from our transactions and experience with you. Finally, we will continue to make certain other disclosures of your nonpublic personal information that are permitted or required by law."[26]

- Cash America's CashNetUSA includes in its description of rights to limit sharing of information: "Please note that even if you Opt-Out, the CashNetUSA Provider may still share Your Information with its Affiliated Companies and Non-Affiliated Third Parties as permitted or required by law. Also, CashNetUSA Provider may share information it collects regarding its transactions and experiences with you with its Affiliated Companies." [27]

Consumer Opt Out Procedures

The Privacy Rule says that financial entities have to provide a "reasonable means" for a consumer to opt out from disclosure of NPI, which can include a form with check off boxes or other reply form, email, online form, or toll-free phone number.[28] Methods used by fringe financial providers range from telling customers that if they used the site, they opted in, to easy to use methods to opt out:

- An online payday loan lead generator's privacy policy opt out rights section states: "You may opt out of receiving communications from us or our third-party partners **by not submitting your information**."[29] (Emphasis added.)
- ACE Cash Express provides a toll free telephone number to call with questions about its privacy policy or to opt out of receiving email.[30] Dollar Financial Group's online privacy policy gives the email address for its Privacy Officer in Canada.[31] Check into Cash provides a toll-free number and a form that can be filled in and mailed.[32] Advance America provides a form to be mailed to its headquarters. Omni Financial Group of Loan Companies provides a mail-in form to opt out of information sharing.[33]

Privacy Policies Do Not Protect Privacy

Just because a company posts a privacy policy, consumers should not be confident that their privacy is actually being protected. California consumers were surveyed by two University of California at Berkeley professors to learn more about their understanding of privacy policies. They found that the majority of Californians believe that privacy policies guarantee the right to require a website to delete personal information on request, a general right to sue for damages, a right to be informed of security breaches, a right to assistance if identity theft occurs, and a right to access and correct data held by the company. A majority of surveyed Californians believed that privacy policies prohibit common business practices such as selling information to a third party or affiliate sharing of customer information. Earlier research found that consumers think privacy policies provide a strong, default set of rules that protect personal information. In other

---

[26] Check 'n Go Privacy Statement (Online), Version Date September 1, 2008.
[27] CashNetUSA Privacy Policy, "Your Right to Limit the Sharing of Your Information," http://www.cashnetusa.com/rivacy_policy.html, viewed 8/10/09.
[28] 16 CFR 313.7(a)(1)(ii)
[29] United Cash Loan Privacy Policy, Section 6, https://unitedcashloans.com/?page=info_privacy, viewed 8/10/09.
[30] ACE Cash Express Privacy Policy, http://www.acecashexpress.com/privacy_policy.php, viewed 8/10/09.
[31] Money Mart Privacy Policy, http://www.loanmart.net/MM/privacy_policy.asp, viewed 8/10/09.
[32] Check into Cash Privacy Policy, obtained from www.checkingtocash.com.
[33] Omni Financial Group of Loan Companies' Privacy Policy, http://www.yesomni.com/misc/privacy_policy, viewed 8/11/09.

words, the term "privacy policy" functions as a "privacy seal of approval" to consumers.[34] As the examples provided above demonstrate, this perception is not accurate.

The new head of the Federal Trade Commission's Bureau of Consumer Protection notes that privacy policies have become useless. A new standard being considered at the FTC is whether businesses' practices violate consumers' dignity, not just the current standard of causing financial harm. In a case decided on Sears' privacy practices, the FTC ruled against the company even though it had a detailed privacy policy.[35]

Fringe Financial Outlet Data Security

Non-bank financial service providers that provide check cashing, payday loans, car title loans, tax preparation and refund anticipation loans, and other fee-for-service financial transactions for low and moderate income consumers collect customer specific information that should be securely handled. Unlike depository institutions which are subject to federal and state regulators' examinations that include data handling and security compliance, store and online financial service providers are lightly regulated, if at all, by state agencies with limited resources. Or, they are subject to the Federal Trade Commission's enforcement of federal requirements, which do not use examination as an enforcement tool.

GLB provides general guidelines that require these companies to develop a written security plan, designate responsible employees, assess risks to customer data, and test and monitor safeguards. Otherwise, security procedures are generally left up to providers. The Federal Trade Commission identified three important security issues: (1) employee management and training; (2) information systems; and (3) managing system failures. Security plans for fringe providers consist of relatively meaningless boilerplate language, such as:

- "ACE restricts access to nonpublic information about you to employees who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information."[36] Advance America payday loan stores have identical language.[37]
- Check 'n Go payday loan outlets use the same statement as ACE but add "Finally, we prevent unauthorized access to your nonpublic personal information by regularly assessing our security standards and privacy policies and by regularly training our employees and requiring our vendors to comply with those standards and policies."[38]
- Nix Check Cashing discloses that "We require all of our employees, outside contractors and businesses who jointly market our products and services to agree in writing to protect the confidentiality of customer information and to use it only for business purposes. Our policy is to prohibit access to your personal information unless there is a

[34] Chris Jay Hoofnagle and Jennifer King, "What Californians Understand about Privacy Online," University of California, Berkeley, September 3, 2008. Abstract at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130, viewed September 2, 2008. Electronic communication from Chris Hoofnagle to author, on file at CFA.
[35] Stephanie Clifford, "Fresh Views at Agency Overseeing Online Ads," *New York Times*, August 5, 2009, www.nytimes.com/2009/08/05/business/media/05ftc.html.
[36] ACE Cash Express Privacy Policy, www.acecashexpress.com/privacy_policy.php, viewed 8/10/09.
[37] Advance America Privacy Policy, www.advanceamerica.net/site-info/privacy , viewed 8/9/09.
[38] Check 'n Go Privacy Statement, https://www.checkngo.com/pdf/privacy.pdf , viewed 8/10/09.

> business reason to do so or we are required by law. We also take other steps to safeguard customer information, maintaining physical, electronic, and procedural safeguards to guard your non-public personal information."[39]

The President's Identity Theft Task Force Report, issued in late 2008, made thirty-one recommendations to address causes and results of identity theft, including educating the private sector on safeguarding data to prevent this crime. As a result, the Federal Trade Commission has held regional seminars for businesses on safeguarding information and composed and distributed improved guidance for private industry. The FTC publication, "Protecting Personal Information: A Guide for Business," reminds businesses to properly dispose of information no longer needed. "Leaving credit card receipts or papers or CDs with personally identifying information in a dumpster facilitates fraud and exposes consumers to the risk of identity theft." The Guidance instructs business to effectively dispose of paper records by shredding, burning or pulverizing them before discarding.[40]

Sample of Consumer Complaints to the Federal Trade Commission

The FTC serves as the national clearinghouse for ID theft complaints and receives consumer complaints regarding non-bank financial services companies' privacy and security practices. CFA filed a Freedom of Information Act request for a small sample of these complaints in mid-2007 to learn more about the types of financial problems that led consumers to contact the FTC. Eight of the sixty-six ID theft complaints in the sample involved credit obtained from financial service companies and alleged that online and retail outlet payday loans as well as refund anticipation loans had been obtained using their stolen information.

CFA also received a sample of complaints filed with the FTC on general credit issues, including Gramm-Leach-Bliley Act, FTC Act, Telemarketing Sales Rule and other credit related issues. Twenty-four of the 190 cases in this sample involved high cost small loan providers. Complaints alleged unauthorized withdrawal of funds from bank accounts and difficulty in stopping repeated withdrawals of funds from accounts. In one case a consumer filled in an online loan application but did not go through with the loan application. However, the lender used the information to access the consumer's bank account to withdraw funds, triggering insufficient funds fees. (See Appendix A for more information on the FTC complaint sample.)

Examples of Privacy and Security Failures at Fringe Financial Providers

Privacy and security policies posted by companies are only as good as their compliance. Following are instances where policy and practice diverge. The most heavily publicized example of the use of stolen identity to obtain a payday loan is no doubt the chief executive of LifeLock whose identity was stolen by a Fort Worth man to get a $500 payday loan in his name. Todd Davis posts his Social Security number on LifeLock's website to advertise their system for safeguarding personal information. Davis told reporters that his identity was stolen because

[39] Nix Check Cashing, http://nixcheckcashing.com/privacypolicy.html, viewed 8/10/09.
[40] Federal Trade Commission, "Protecting Personal Information: A Guide for Business," at 21, www.ftc.gov/bcp/edu/pubs/business/idtheft/bus69.pdf.

Teletrack, the specialty screening service used by payday lenders, doesn't receive fraud alerts from Experian, TransUnion and Equifax.[41]

The **Texas** Attorney General has brought cases against payday lenders and other retailers for improperly disposing of consumers' personal financial information. In 2008, the Attorney General settled a case with CNG Financial Corp and its subsidiaries Check 'n Go of Texas, Inc., and Southwestern & Pacific Specialty Finance, Inc. involving claims the company "recklessly disposed of consumers' financial information."[42] The case, initiated in May 2007, charged that several Check 'n Go outlets in Texas threw customer files in the trash. The files contained names, addresses, Social Security numbers, drivers' license numbers, employment information, and bank account numbers and bank routing numbers. The payday lender kept copies of loan applications, Truth in Lending Disclosure statements, customers' checks and documents containing identification information. The stores also kept customers' thumbprints. The Texas complaint states, despite company claims to safeguard personal information and promises to shred borrowers' checks, "Specifically, Defendants fail to protect and safeguard from unlawful use or disclosure, consumers' sensitive personal information which is collected or maintained by Defendants in the regular course of business. Because these unlawful practices expose Defendants' customers to the risk of identity theft, these proceedings are in the public interest."[43] To settle the case, Check 'n Go agreed to upgrade its security program and pay $220,000 to fund enforcement of the Texas Identity Theft Enforcement and Protection Act.[44]

Texas officials also brought charges against EZPAWN for failing to protect customer records containing sensitive personal information and systematically exposing customers to identity theft. Attorney General's Office investigators found that several San Antonio EZPAWN stores disposed of customer records in public trash receptacles behind the stores. The records included names, addresses, Social Security and driver's license numbers and checking account information.[45] The complaint filed by the Attorney General listed the sensitive personal financial information collected by EZPAWN, including employer information, contact information for references, recent bank statement, phone bills, valid driver's license or state photo identification, proof of income by way of a pay stub, and a voided check from the consumer's checking account.[46] The files were not shredded or otherwise made unreadable.

The **Texas** complaint against EZPAWN charged the company for deceptively advertising a protective privacy policy: "By representing to consumers that DEFENDANTS' Privacy Policy protected consumers' financial privacy, DEFENDANTS misled consumers and caused confusion

---

[41] Pamela Yip, "But LifeLock chief keeps his data public; FW man admits guilt," *The Dallas Morning News*, July 24, 2007.
[42] Chris Rizo, "Check 'n Go settles case over its records handling," LegalNewsline.com, http://www.legalnewsline.com, viewed May 12, 2008.
[43] State of Texas v. CNG Financial Corporation, Check 'n Go of Texas, Inc., and Southwestern & Pacific Specialty Finance, Inc., Plaintiff's Original Petition and Application for Temporary and Permanent Injunction, filed May, 2007, at 4.
[44] *Ibid.*
[45] Press Release, "Attorney General Abbott Cracks Down on Identity Theft; Takes Action Against Pawn Shop Chain for Exposing Records," May 8, 2007, http://www.oag.state.tx.us/oagNews/release.php?print=1&id=1999, viewed May 9, 2007.
[46] State of Texas, v. Texas EZPAWN L.P. d/b/a EZMONEY Loan Services, Inc., et al, Plaintiff's Original Petition, District Court Bexar County, TX, filed May 8, 2007, at 7.

regarding the protection and security used to protect the sensitive and personal identifying information which DEFENDANTS required consumers to provide to them…"[47] Final judgment in the case, reached in 2008, required EZPAWN and EZMONEY to overhaul information security programs and pay $600,000 to the State of Texas to fund identity theft investigations. In addition to staff training, notices to consumers were to be posted in stores.[48]

An **Illinois** Check into Cash store apparently discarded boxes of unshredded loan records in a nearby trash bin in 2007. The boxes contained loan documents, account registers, collection notes, customer history reports and customer information sheets, including Social Security numbers, addresses, photocopies of driver's licenses. News reports noted that this handling of customer information violated the company's policies and that the responsible employee had been fired.[49]

A manager at a **Virginia** Check 'n Go outlet sent an anonymous letter, shared with all members of the Virginia General Assembly in August 2007, that detailed insecure handling of customer files. The letter alleged that store managers were instructed to dispose of customer files in unlocked public trash receptacles. The manager also described the routine practice of contacting the borrower's bank, using account numbers and PINs to impersonate the borrower in order to learn when funds were available in the account to repay the loan. The manager noted use of bank account transaction information to intimidate borrowers.[50]

A **Florida** check cashing outlet reportedly disposed of job applications containing Social Security numbers and other personal information in an insecure manner. A plastic bag containing job applications which were supposed to be shredded was found at a fast food restaurant a mile from the check cashing outlet.[51]

Idaho Department of Finance settled a 2005 case with Check 'n Go of Idaho, Inc. with an assurance that the payday lender would reform its customer information handling practices. Inspectors found that the company collected customers' checking account PIN numbers without their knowledge or consent. During the loan application process, borrowers were asked to input PIN numbers into the lender's telephone key pad, which were then electronically retrieved and stored for future account balance verification. Idaho regulators required Check 'n Go to discontinue this practice, alert customers to change their PINs, and to purge written or electronic records of customer PIN numbers obtained without authorization or consent. The company paid a $50,000 administrative penalty and investigative fee to the Idaho Department of Finance.[52]

---

[47] *Ibid*, at 9.
[48] Press Release, "EZ PAWN, EZ Money required to improve privacy safeguards," Texas Office of Attorney General, June 24, 2008.
[49] Christine Des Garennes, "Papers with personal info found in Check into Cash's trash," *The New-Gazette*, Champaign, Illinois, May 23, 2007.
[50] Emailed letter from Check 'n Go manager to Virginia General Assembly, August 6, 2007, on file with CFA.
[51] "Bag Full of Job Applications Found in Parking Lot," WFTV.com, Orange County, Florida, posted July 9, 2007. http://www.wftv.com/, viewed July 17, 2007.
[52] Press Release, "Idaho Department of Finance Obtains Assurance of Discontinuance From Check 'n Go of Idaho," January 25, 2005, viewed at http://spokane.bbb.org/alerts/alerts.html?newsid=575&newstype=1, viewed August 13, 2007. Also see State of Idaho, Department of Financial, Consumer Finance Bureau vs. Check 'n Go of Idaho, Inc., Assurance of Discontinuance, Docket No. 2004-6-10, January 19, 2005.

Washington Department of Financial Institutions also took enforcement action against Check 'n Go of Washington for mishandling customer information. Regulators inspected stores in three cities and found that Check 'n Go obtained and stored the PIN numbers of payday loan borrowers without notice or consent. The Department's Statement of Charges against the company noted that "Respondent Check 'n Go's unauthorized gathering and retention of consumer's PIN numbers unnecessarily exposed the affected consumers to possible theft of funds and possible identity theft." The Statement also noted that a PIN number is an 'access device' under Washington law. "Exerting unauthorized control over or possessing an access devise can constitute the crimes of Theft in the Second Degree or Possession of Stolen Property in the Second Degree pursuant to RCW 9A.56.020, .040, and .160; both of which are class C felonies."[53] Although DFI threatened to revoke the company's license, the case which involved multiple violations was settled with a consent order in December 2006. The fine was $82,000 plus restitution of $69,675 and an investigative fee. The company agreed to comply with the law and discontinue all practices raised in the Statement of Charges.[54]

A **Montana** car title lender reportedly disposed of boxes of customer records when it closed its doors in Anaconda in 2007. The police received reports of people "dumpster diving" and looking at Title Cash files which contained names, addresses, phone numbers, Social Security numbers, and loan details including checkbook carbon copies showing loan amounts and dates for payday and car title loans. Police accumulated about fifteen months of records. The company denied disposing of records improperly but sent a letter of apology to customers and recommended placing a fraud alert on credit reports. A customer shared the company's privacy policy with a reporter. The Privacy Notice said: "We restrict access to non-public personal information about you to those employees who need to know that information to provide products and services to you. In addition, we maintain physical and procedural safeguards that comply with federal standards to guard your information."[55]

Payday Loan Privacy and Security Issues

Payday loan design adds privacy and security risks in addition to usurious interest rates and debt traps for borrowers. Every payday loan involves the borrower providing a signed personal check made payable to the payday lender for the loan amount plus the finance charge. This check is held in the payday loan office until the loan is due on the borrower's next payday. Either the check is then deposited to collect payment on the loan, or, as more often happens, the borrower returns to the outlet to "buy back" the check by repaying the loan with cash. Payday lenders hold either a paper check drawn on the borrower's bank account as security for the loan or the bank account number, routing number, and authorization to electronically access the borrower's bank account to repay the loan. They may hold both. This means that payday loan

[53] Washington Department of Financial Institutions Statement of Charges, Check 'n Go of Washington, Inc., DBA Check 'n Go, No. C-05-012-06-SC01, filed August 2, 2006.
[54] Washington Department of Financial Institutions, Consent Order, Check 'n Go of Washington, Inc., d/b/a Check 'n Go, No. C-05-012-06-CO01, December 8, 2006.
[55] Kathie R. Miller, "Title Cash issues apology," *Anaconda Leader*, April 20, 2007; "Police ask for assistance in Title Cash Investigation," *Anaconda Leader*, May 30, 2007. Jim Tracy, "Title Cash records investigation widens," *Anaconda Leader*, April 6, 2007. Jim Tracy and Kathie Miller," Payday loan company leaves confidential records in trash," *Anaconda Leader*, April 4, 2007.

stores and online lenders have in their records all the information needed to steal a consumer's identity or to make unauthorized withdrawals from a consumer's bank account.

Consumers are at risk of new or existing account fraud when their identities are stolen and crooks get credit and debit card numbers or the information needed to open new credit accounts. Federal law sets liability limits to protect consumers from unauthorized credit and debit card expenditures. For credit cards, the Truth in Lending Act limits liability to $50 for an unauthorized charge while the Electronic Fund Transfer Act limits liability for unauthorized debit card use on a sliding scale, depending on how quickly consumers notify the bank. The same clear limits do not apply to paper checks, making consumer information held by check cashers and payday lenders an important concern for consumers. State uniform commercial codes (UCC) do not provide a right of recredit, a liability limit, or a federal agency to handle consumer complaints. For transactions that start as a paper check but are later converted to electronic presentment, UCC applies, not the Electronic Fund Transfer Act. Even when a payday loan is secured by a debit authorization and is covered by EFTA, the federal law's ban on requiring electronic payment as a basis for extending credit does not clearly apply to a single payment transaction.[56]

The president of the Electronic Payments Network, the largest private check processing system, told the Washington Post in 2004 that one of the most dangerous things a consumer can do on a Web purchase when they are dealing with someone they had no prior relationship with is give out a bank account number. He noted that using a credit card for purchases provides more consumer safeguards and doesn't give crooks access to financial assets.[57] Yet every payday loan application involves giving out a bank account number to a stranger.

Online lenders have used bank account information provided by consumers in applying for a loan to also charge consumers for an unrelated product. The Federal Trade Commission filed a complaint against a seller of twenty-two or more prepaid debit cards. The same company also operated online loan websites, such as www.SuperAutoSource.com, www.SuperCashSource.com, and www.FastCashUSA.com. The FTC complaint alleged that the company debited, without authorization, a $159.95 "application and processing" fee from consumers' bank accounts. The company used either the Automated Clearing House Network (ACH) or remotely created checks (demand drafts) to withdraw funds from consumers' accounts. In some cases, consumers who had applied for payday loans and had not applied for the prepaid debit card had the fee deducted from their bank accounts. In applying for online loans, consumers were required to provide the bank account information, social security number, and driver's license number. Consumers learned about the fee when they saw their bank statements or found out they had overdraft charges for insufficient funds. In settling the case, EDebitPay, LLC, and other parties, agreed to pay $2,258,258 to consumers who lost money in the scheme, to stop making misrepresentations, and to get clear consumer consent before debiting an account.[58]

---

[56] Electronic Fund Transfer Act, 1693k. Compulsory use of electronic fund transfers.

[57] Caroline Mayer, "Keep Close Watch on Bank Accounts," *Washington Post*, July 19, 2004, A-8.

[58] Federal Trade Commission, "Online Marketers of Prepaid Debit Cards to Subprime Consumers Will Pay More than $2.2 Million to Settle FTC Charges," January 24, 2008. http://www.ftc.gov/opa/2008/01/cards.shtm. See, also, FTC v. EDebitPay, LLC; EDP Reporting, LLC; EDP Technologies Corporation; Secure Deposit Card, Inc.; and Dale Paul Cleveland and William Richard Wilson; Defendants; Complaint for Injunctive and Other Equitable Relief, United States District Court Central District of California, CV-07-4880, filed July 20, 2007.

The Federal Trade Commission settled a similar case in mid-2009 with a debit card company that used bank account information provided by consumers to apply for online payday loans to take money from consumers' bank accounts for a debit card they did not knowingly order. The FTC alleged that thousands of consumers were charged $39.95 to $54.95 for a prepaid card with no funds loaded on the cards when they applied for payday loans online. Consumers who clicked a button to apply for a loan also bought the debit card. The defendants were VirtualWorks, LLC, a/k/a Virtual Works, d/b/a EverPrivate Card and Secret Cash Card and Swish Marketing, Inc. and several officers. VirtualWorks marketed its EverPrivate Card through affiliates that typically displayed an offer for the card on websites that market payday loans. Swish was VirtualWorks' highest yielding marketing affiliate, according to the FTC complaint.[59]

A Wisconsin TV station reported that a payday lender sold borrowers' personal bank information to Roadside Plus, a company that withdrew $21.95 every month from consumers' bank accounts with the transactions identified on bank statements only as an 800 number.[60]

Even applying for an online payday loan can result in unauthorized deductions from consumers' bank accounts. A Tennessee couple applied for but was turned down for an online payday loan. However their bank account information entered on the loan application was used to deduct payment of $39 month after month to pay for ID theft insurance that the customers had not requested. In order to stop the deduction of the funds, they had to close and reopen a bank account.[61]

In some cases, information is manufactured to apply for payday loans. Chandler, Arizona, police arrested a group of people who used manufactured pay stubs and low balance bank accounts to obtain payday loans. The leader of the ring would recruit accomplices who opened checking accounts in their own names and then used phony pay stubs to get loans that were split with the ring leader. In searching the leader's vehicle, police found a briefcase full of checks, identification, and fake company documents in his name.[62]

Payday Loan Check-Holding Design Harmful to Borrowers

Loans based on unfunded checks held by lenders until payday cause other problems for cash-strapped borrowers. Check holding makes the lender the first priority for payment out of the borrower's next paycheck. Failure to repay results in bounced check fees from the payday lender and imposed by the borrower's bank. It also results in a negative report to credit reporting services used by banks and retailers in deciding whether to accept payment by check or to open an account. Consumers can lose their check-writing privileges at retailers or become black-listed on ChexSystems, unable to open a new bank account due to bounced checks triggered by payday lending.

---

[59] Press Release, "FTC Settlement Bars Deceptive Online Marketing Tactics; Payday Loan Applicants Were Charged for Unwanted Debit Cards," Federal Trade Commission, August 20, 2009, http://www.ftc.gov/opa/2009/08/everprivate.shtm.

[60] "Bank Account Scam," 15 WMTV, Madison, WI, March 28, 2006. http://nbc15.madison.com/news/headlines/2539516.html, viewed March 29, 2006.

[61] "Couple Turned Down for Loan, Charged for Unwanted Service," 6WATE, Dandridge, TN, April 2, 2008, http://www.wate.com/global/story.asp?s=8106140&ClientType=Printable, viewed April 3, 2008.

[62] Devin Hicks, "Police uncover payday loan scam," *The Arizona Republic*, July 20, 2007, http://www.azcentral.com/community/chandler/articles/0720abrl-fraud.html, viewed July 24, 2007.

Payday lenders who use debit authorization as security for a loan and as the payment method for a loan get direct access to the borrower's bank account when pay or benefits are deposited on payday. As soon as funds are deposited, the payday lender can withdraw payment. Repeat presentment of the check or debit for payment can trigger multiple NSF fees for consumers with low balances.

A sailor based in Florida was charged $200 for ten returned check fees as a result of repeated attempts to debit his account to collect on one payday loan. His credit union charged $20 per returned debit as did the payday lender. The original $300 loan cost a $45 finance charge and 342.19% APR and listed the personal check presented electronically as "security" for the loan.[63]

Loans based on writing unfunded checks have an adverse effect on consumers' bank account ownership. Recent research by the Harvard Business School found that access to payday loans is associated with higher numbers of involuntary account closures where a bank closes a customer's account because it has been repeatedly overdrawn.[64]

Check holding also fosters coercive collection tactics when lenders threaten criminal sanctions for failure to "make good" on the check used to secure the loan.[65] Checks as security for loans give an advantage to the payday lender for payment. By holding the borrower's check, lenders get the ability to call the consumer's bank to check "funds availability." As soon as the bank tells the lender funds are available to cover the check, the lender can go to the bank to collect on the payday loan. Consumers who are juggling bill payment decisions lose all control over the timing for repaying a payday loan, since the lender can deposit the loan check at any time after the due date, precipitating NSF fees for other checks written. For example, the payday lender's decision about when to put through the check may cause the rent or mortgage check to bounce. Some lenders have required multiple checks for a single loan, maximizing the number of NSF fees that were charged when the loan was not repaid in full on the borrower's next payday.

Consumers lose control of their checking accounts when lenders condition the extension of credit on direct electronic access, as well. While a borrower can stop payment on a paper check, the same right does not apply by law for a single debit. Consumers may ask their bank to revoke authorization for lenders to electronically withdraw funds, but savvy lenders can easily evade those efforts. A lender can too easily avoid a stop order on an electronic payment simply by breaking an electronic withdrawal into smaller segments or altering the amount by a few pennies to evade the description of the transaction in the stop order. As a result, consumers are confronted with multiple NSF fees when the payday lender makes multiple attempts to electronically withdraw funds from the consumer's checking account. For example: An Indiana consumer had insufficient funds to repay a $300 payday loan plus $35 finance charge on its due date. The lender's first electronic funds draft was returned for insufficient funds. The lender then broke the debt into three parts and submitted three electronic drafts for $167.50, $167.50

[63] Loan and credit union documents on file with Consumer Federation of America.

[64] Dennis Campbell, Asis Martinez Jerez, and Peter Tufano (Harvard Business School). "Bouncing Out of the Banking System: An Empirical Analysis of Involuntary Bank Account Closures." June 6, 2008. Available at: http://www.bos.frb.org/economic/eprg/conferences/payments2008/campbell_jerez_tufano.pdf

[65] CFA Testimony, Federal Trade Commission Workshop on Fair Debt Collection Practices Act, June 20, 2007.

and $20, respectively. The borrower's bank charged a $26 "bounce protection" charge for each item which overdrew his account.[66]

Payday loans using repeat debit authorizations facilitate loan renewals (which lead to repeated payment of a high loan fee directly from the consumer's checking account) much more easily than loans based on presenting paper checks for payment. Online payday loans, all of which use debit authorization, frequently set loans up to automatically renew every payday with just payment of the finance charge withdrawn from the borrower's account by electronic fund transfer.

For example, for an initial loan of $200, the consumer authorizes a debit of $260 from her account two weeks from the date of the loan. Unless the consumer faxes a request three days in advance of the due date, two weeks after the initial loan the lender will deduct the $60 finance charge and renew the $200 loan for another pay cycle. Two weeks later, an additional $60 is debited and the $200 plus another $60 fee is still due two weeks after that. This cycle can continue for many weeks. The consumer has $120 withdrawn from his or her checking account in every four week period without reducing the loan balance of $200.[67]

Payday Loan Design Exposes Others to ID Theft Risks

The only prerequisites for obtaining a high cost payday loan are showing identification, a bank statement, and a paystub to show that the applicant has an open bank account and a source of income that is deposited into that bank account. When obtaining a payday loan at a store, borrowers provide a personal check, written for the amount of the loan and the finance charge, which the lender holds until the borrower's next payday before presenting it to the bank for payment. Lenders do not automatically verify that the loan applicant matches up with the bank account information provided. In selling its data service, one provider noted that "a lot of employees simply just don't verify as they should, costing managers, owners and companies untold amounts of bottom-line loss."[68] Online payday lending is all conducted via websites and email, with loans delivered and repaid through electronic access to borrower's bank accounts. Lax information handling practices leave innocent consumers exposed to ID theft victimization.

Identity theft by people who have access to personal financial information has resulted in loans being extended based on stolen identities but leaving the ID theft victim on the hook for collection attempts and to correct credit reports. In other cases, thieves have fabricated identities to apply for loans. Some examples:

---

[66] On file with CFA.

[67] Jean Ann Fox, "Internet Payday Lending," Consumer Federation of America, November 2004, http://www.consumerfed.org/pdfs/Internet_Payday_Lending113004.pdf .

[68] "DATATrue: Embracing Change and Improving the RTO Bottom Line," RTO Online, March 12, 2008, http://www.rtoonline.com/Content/Article/Mar08/DataTrue Change031108.asp, viewed March 12, 2008. DATATrue says it provides clients the ability to verify accuracy of its prospective customers' name, address, phone number, employer's address and phone number, Social Security number, date of birth, bank account routing verification, bank account number verification, bank account status (open and active), and to confirm a positive relationship between the bank and the client. http://www.datatrue.net/datatrue.php, viewed March 12, 2008.

- A used car salesman was convicted of aggravated identity theft and credit card fraud for using stolen identities of his customers to apply for credit in the victims' names. In addition to opening credit cards, the former salesman created phony payroll checks used to obtain payday loans. Victims learned of the crimes when the unpaid loans were listed on their credit reports.[69]

- A Houston, Texas man was contacted by a debt collector, looking for someone with his name, Social Security number and driver's license but listed as living in Austin. Apparently his identity had been stolen and used to open a bank account in Austin into which paychecks were deposited for a few months to build up a deposit history. Then the ID thief used that bank account to apply for and obtain about $10,000 in payday loans.[70]

- The Louisiana State Police arrested former employees of a national mail-order pharmacy who allegedly stole the personal information of customers to apply for payday loans across the country. At the time of their arrest, State Police detectives had identified 26 victims ranging in age from five years old to senior citizens whose personal information was used in applications for 120 loans.[71] Some of the victims were friends and family members. Charges filed included identity theft, computer fraud, access device fraud and theft of business records.[72]

Consumers can easily be the victims of debt collection attempts caused by unauthorized payday loans when others steal or use their personal information to obtain loans in their names, with the loan proceeds going elsewhere. An Alabama woman was arrested in late 2008 for allegedly stealing another woman's identity to apply for loans. She was charged with felony identity theft, second-degree felony forgery and a count of misdemeanor negotiating a worthless check. The woman used a family member's Social Security number, birth date and information to obtain payday loans from Speedy Cash, get a mortgage, and write forged checks. The local police told a reporter that they get at least three such reports every week.[73]

In another case of unauthorized use of personal information to obtain payday loans, an employee of an ACE Cash Express in Tyler, Texas, was suspected of using information from a check cashing customer to take out a $1,203.80 loan. The ID theft victim took the case to the local police department which told reporters the number of potential cases was "substantial."[74] In a similar case, the manager of the Shreveport, LA "Money in a Flash" payday loan outlet was arrested for allegedly making 21 fraudulent payday loans. She was accused of using the personal

---

[69] "Washington man sentenced for credit card fraud and identity theft," Missoulian.com News Online, April 18, 2008, http://www.missoulian.com/articles/2008/04018/bnews/br88.prt, viewed April 21, 2008.
[70] Loren Steffy, "ID theft nightmare as a reality," *Houston Chronicle*, December 17, 2005.
[71] "Identity Theft Ring Arrested in La.," Insurance Journal, July 19, 2007.
http://www.insurancejournal.com/news/southcentral/2007/07/19/81921.htm, viewed July 20, 2007.
[72] "Police Arrest Women in Identity Theft," *The Advocate*, July 19, 2007,
http://www.2theadvocate.com/news/8588547.html, viewed July 20, 2007.
[73] "Enterprise Woman Nabbed for Identity Theft," *The Enterprise Ledger*, November 29, 2008, viewed at
http://www.tradingmarkets.com/print.site/news/Stock%20News/2055495, viewed November 30, 2008.
[74] "ID Theft Suspected at Check Cashing Store," KLTV, 7, September 19, 2006.

information of prior customers to obtain new loans, then generating counterfeit checks to make pseudo payments on the loans.[75]

A multi-jurisdiction case of online payday loan identity theft occurred in Austin, Fort Bend, Brazoria, and Harris County, Texas. In mid-2008, thirty-eight people were arrested for stealing identities and getting online payday loans in the victims' names. According to news reports, people were recruited to open bank accounts to receive direct deposit of online payday loan proceeds. Apparently, hundreds of personal identities were stolen between December 2006 and February 2008 from patient records at an institution where some of those arrested were employed. The loans ranged in size from $200 to $800 and, once deposited, suspects would withdraw the entire balance and permit the account to go dormant. The loan companies sent collection letters to people in whose names the loan accounts were opened but who had not applied for or received the loans. The payday lenders contacted law enforcement officials and stopped efforts to collect from the ID theft victims. Fort Bend County officials estimated that $230,000 was stolen in this scheme involving more than five hundred stolen identities and 1,000 loans.[76]

A federal grand jury handed down indictments of three Chicago area residents charged with wire fraud and ID theft for stealing $70,000 by using stolen personal information to apply for payday loans. A contract worker at AT&T allegedly stole Social Security numbers and personal data from 2,100 AT&T employees and used the information to take out $70,000 in $1,000 loans online. ID theft victims only became aware that loans had been made in their names when debt collectors made contact and credit ratings were damaged. Many of the loans were made through PaydayOne, a Texas online payday loan company. Although loans were applied for using stolen identities and fabricated documentation, the loan proceeds were direct deposited into accounts controlled by the alleged ID thieves.[77]

In 2009, a clerk in the financial-litigation unit of the U. S. Attorney's Office in Philadelphia pleaded guilty to fraud and aggravated identity theft. She reportedly used people's personal information gleaned from government computers to obtain $34,435 in online payday loans over a three year period.[78] A Lancaster County, Pennsylvania man will reportedly plead guilty to conspiring to use personal information from drunken-driving defendants' court records in an identity-fraud scheme to open bank accounts and take out payday loans in victims' names.[79]

Apparently, online payday lenders' screening processes do not match up loan applicant information with the ownership of the bank account into which loan proceeds are deposited. The

---

[75] John Andrew Prime, "Shreveport police arrest woman for forgery," *The Shreveport Times*, August 3, 2006.
[76] Eric Hanson, "38 accused in identity theft scheme," *Houston Chronicle*, July 24, 2008, http:www.chron.com/disp/story.mpl/front/5906582.html, viewed July 25, 2008; Mary Hogan, "Arrests made in ID theft case," *Sealy News*, September 23, 2008, http://www.sealynews.com/articles/2008/09/23/news/news04.prt, viewed September 25, 2008; Don Munsch, "38 indicted in massive ID theft ring," *Fort Bend Herald*, July 25, 2008, http://www.fbherald.com/articles/2008/07/25/news/doc488a2c53e1cb7089352438.prt, viewed June 2, 2009.
[77] Jeff Coen, "Identity thieves use payday loans to make a quick buck, authorities say," *Chicago Tribune*, July 21, 2009. See also Chuck Miller, "AT&T temp indicted in ID theft scheme," *SC Magazine US*, July 13, 2009.
[78] Allison Steele, "Ex-worker in U.S. Attorney's Office guilty of fraud," philly.com, September 12, 2009, http://www.philly.com/philly/news/pennsylvania/20090912_Ex-worker_in_U_S_Attorney_s_Office_guilty_of_fraud.html, viewed September 14, 2009.
[79] Associated Press,"Man Charged with ID theft targeting DUI defendants," The York Daily Record, September 15, 2009.

Federal Trade Commission's Red Flag Rules, required under the Fair and Accurate Credit Transactions Act and intended to prevent this type of new account fraud, will finally be enforced starting in November 2009. (For more information on the FTC Red Flags Rule, see Handbook, section C.)

Debt Collection Calls for Phony Payday Loan Debts

Consumers are being harassed for collection of payday loans they never got, apparently as a result of misappropriated personal information. The West Virginia Attorney General warned consumers in 2008 about scammers masquerading as debt collectors and law enforcement officials to bilk consumers out of loan payments they did not owe. Collectors, operating under names such as U.S. National Bank, Federal Investigation Bureau, and United Legal Processing, repeatedly called people at home and at work and threatened arrest if they didn't pay supposed debts. Consumers who took out online payday loans in the past were targeted. West Virginia officials stated that the group stole consumers' Social Security numbers and other personal information from payday lending websites.[80] The FBI told a Pittsburgh reporter that fraudsters can easily hide their tracks by hopping through computers located throughout the world, making it very difficult for authorities to identify and stop abusive collection of nonexistent debt.[81]

The Better Business Bureau (BBB) issued a national alert about phony debt collectors that call consumers and threaten arrest for failure to repay payday loans they had not gotten. In this 2009 case, the callers claim to be lawyers with the "Financial Accountability Association" or the "Federal Legislation of Unsecured Loans," and use the victims' personal information to frighten them into making payments on nonexistent loans. The BBB has raised the possibility that a data breach put consumer information, such as Social Security numbers, bank account numbers or driver's license numbers into the hands of callers. Consumers are accused of defaulting on a payday loan and are told they are being sued. If the victims refuse to wire up to $1,000 or turn over current bank account information, they are threatened with arrest.[82]

Remotely Created Checks Deprive Consumers of Federal Protections for Bank Accounts

Many online payday loan contracts include authorization to collect payment through creation of a "remotely created check" – a payment device that is prone to fraud and has largely been discredited. These are "demand drafts," in which a creditor creates a paper check that withdraws funds from a consumer's bank account without the consumer seeing or signing the instrument. The legal theory is that the consumer has authorized the creation of a check, perhaps even orally, without ever signing a check. This method of payment is highly prone to abuse.[83]

---

[80] Press Release, "Attorney General McGraw Warns Public of Fake Internet Loan Collectors Impersonating Law Enforcement Officers and Extorting Money from Consumers," West Virginia Office of Attorney General, August 12, 2008. See, also, Alice Gomstyn, "Fake Debt Collectors Terrify Consumers," ABC News, August 21, 2008, viewed at http://abcnews.go/com.

[81] "Call 4 Action: Scam Artists Try to Collect Debts Over Phone," ThePittsburghChannel.com, August 25, 2008.

[82] Press Release, "Widespread Harassment from Phony Debt Collectors Raises Concerns of Mass Data Breach," Better Business Bureau, August 3, 2009.

[83] The Federal Trade Commission settled four cases for $16 million that involved telemarketers and Wachovia Bank which involved the use of demand drafts to withdraw unauthorized funds from consumers' accounts. The complaint alleged that the defendants had illegally purchased leads containing consumers' unencrypted bank account numbers for use in telemarketing. (FTC Press Release, January 13, 2009).

Applications for a payday loan to be repaid by demand draft require consumers to provide their bank account routing number and other information necessary to create a demand draft as well as to sign a boiler plate contract to authorize the device. No paper check is involved in the transaction. The account information is initially used by online lenders to deliver the proceeds of the loan into the borrower's bank account using the Automated Clearing House (ACH) system[84]. Once the lender has the checking account information, however, he can use it to collect loan payments via remotely created checks even after the consumer revokes authorization for the lender to electronically withdraw payments. Some complaints in the FTC FOIA sample involved repeated withdrawals of funds by payday lenders. (See Appendix A.)

The use of remotely created checks is common in online payday loan contracts. For example: the ZipCash LLC "Promise to Pay" section of a contract included the disclosure that the borrower may revoke authorization to electronically access the bank account as provided by the Electronic Fund Transfer Act. However, revoking that authorization will not stop the lender from unilaterally withdrawing funds from the borrower's bank account. The contract authorizes creation of a demand draft which cannot be terminated. "While you may revoke the authorization to effect ACH debit entries at any time up to 3 business days prior to the due date, **you may not revoke the authorization to prepare and submit checks on your behalf until such time as the loan is paid in full**." (Emphasis added.)[85]

In a variation on the remotely created check payment method, MTE Financial Services, Inc. d/b/a Cash Advance Network includes the following provision in its Authorization Agreement for Preauthorized Payment: "However, if you timely revoke this authorization to effect ACH debit entries before the loan is paid in full, you authorize us to collect the payments due by using your debit card information that you provided to us on your application (this will be done as a POS transaction). This may be done in one or multiple amounts using various debits until the amount you owe is paid in full."[86] The same lender will take funds from any bank account the borrower has if the one listed to obtain the loan is closed or contains insufficient funds.[87]

Use of a demand draft to secure a payday loan and to collect payment on a payday loan undermines existing consumer protections in the payment system. Consumers have the right under EFTA to revoke the authorization to pay the loan through electronic withdrawals from their bank accounts. However, consumers who exercise that right will still have no control, other than closing their account, over continued withdrawals using remotely created checks. A key protection missing for demand drafts is the right to get a "recredit" within ten business days after a consumer notes and reports an unauthorized transaction.[88]

A Washington consumer filed a complaint with the Department of Financial Institutions about an online payday loan from Cash Advance, based in Carson City, Nevada. The borrower reported

---

[84] ACH transactions are widely used and are subject to rules adopted by the National Automated Clearing House Association (NACHA), an industry self-regulatory body. Use of bank account information obtained for an ACH transaction to create a demand draft is not covered by NACHA rules.
[85] Loan Supplement (ZipCash LLC) Form #2B, on file with CFA.
[86] MTE Financial Services, Inc. "Authorization Agreement for Preauthorized Payment," October 10, 2008, on file with CFA. The loan of $300 cost $90 in finance charges and had a disclosed APR of 842.308%.
[87] MTE Financial Services, Inc. "Loan Note and Disclosure," October 9, 2008, on file with CFA.
[88] "Telephone Check? Could the Wachovia 'demand draft' problem happen to you?" Consumers Union blog post, February, 6, 2008. http://www.consumersunion.org/blogs/fpn/2008/02/telephone_check_could_the_wach_1.html

faxing a letter to the lender in an effort to set up a repayment plan which reportedly the lender accepted. In Washington, consumers are provided the right to set up a payment plan prior to defaulting on a loan. The borrower alerted her credit union that she had revoked authorization to withdraw the full loan payment from her account.[89] Since the borrower had revoked electronic access to her account, the lender converted the ACH authorization to a paper check with a fictitious check number and used the remotely created check to withdraw $480 from the borrower's bank account. The consumer reported that this unexpected withdrawal caused great hardship and she was unable to buy food or pay bills.[90]

An added layer of fraud concern about remotely created checks stems from processing demand drafts electronically via the Check 21 process where no paper check was involved in the transaction. Anyone with a consumer's bank account number, routing number and other information typically provided on an Internet payday loan application can create an electronic file which can be formatted into files that will be processed through image-exchange networks. This electronic processing of remotely created "checks" (RCCs) clears faster, making it harder for consumers to take action to control payments out of their accounts.[91]

A Federal Reserve Bank of Atlanta official noted last year that remotely created checks should not be processed as Check 21 items and noted that the Federal Reserve has no idea how many of these payments are in the system. An industry expert noted that RCCs are too dangerous to allow, since banks sometimes fail to do due diligence on merchants and because there is no automated method to track these transactions.[92]

Permitting a lender to write a check to withdraw funds from the consumer's bank account exposes borrowers to fraud, deprives consumers of dispute rights for unauthorized debit transactions under EFTA, leaving a victim on her own to sort out the charges and resulting insufficient funds and overdraft fees from other payments that are returned unpaid due to presentment of the demand draft. The Federal Reserve enacted a requirement in 2005 that changed the warranty for demand drafts from the consumer's bank to the financial institution that accepted the demand draft for deposit. This action, while positive, provides little consumer protection from unauthorized withdrawal of funds from checking accounts by anyone possessing simple bank account information.

Tax Return Preparation and Filing Privacy and Security Issues

Filing tax returns every year is a legal requirement for all Americans with taxable income or who are claiming federal benefits delivered through the tax refund system, such as the Earned Income

---

[89] Borrower letter to online payday lender, dated August 19, 2004, included with complaint filed with Washington Department of Financial Institutions. The borrower reported that the fax number given by the lender did not work.
[90] Complaint filed with the Washington Department of Financial Institutions, September 10, 2004, identity of borrower redacted. Complaint includes copies of letter to lender, copy of remotely created check front and back. On file with Consumer Federation of America.
[91] MyECheck claims to be the first Check 21 solution for remotely created checks and markets these electronic RCC transactions as safer for the merchant than ACH because the Uniform Commercial Code has no chargeback rights. See: http://www.myecheckcorporate.com/alternativepayment/28.html, viewed May 21, 2009.
[92] "Remotely Created Checks Linked to Image Exchange Stoke Fraud Fears," Digital Transactions News, June 26, 2008, http://www.digitaltransactions.net/newsstory.cfm?newsid=1825, viewed May 21, 2009.

Tax Credit provided to working poor citizens. Preparing and filing tax returns at commercial outlets and the related sale of tax-related financial services products poses privacy and security issues for consumers. Tax returns contain all the information needed for an identity thief to facilitate new and existing account fraud. The information contained in a tax return is also valuable for targeted marketing of other products and services. And, tax return information is shared with banks to deliver high cost refund anticipation loans (RALs). The rules that apply to the use of tax return information are governed by the Internal Revenue Service code and IRS regulations but only apply to tax preparers, not to the third-parties with whom they share information. (See Handbook Section IX.)

Taxpayers share their most sensitive personal and financial information with their tax preparers and expect that information to be safeguarded. Lack of supervision of tax preparers means that trust can be misplaced. A few years ago the U.S. Public Interest Research Group (PIRG) surveyed tax preparation booths located in large retail outlets to see if taxpayer information was shielded from public view as staffers prepared returns. PIRG surveyors visited fourteen stores in nine states. In three instances surveyors were able to easily read private information on forms by walking by booths or standing nearby in public areas. In nine of fourteen stores, surveyors could read computer screens showing nonpublic personal information from public areas. In the four cases where tax preparation booths were adjacent to food courts, surveyors could easily sit for extended periods to listen and observe personal information.[93] Shoulder "surfing" is one of the methods used to steal consumers' identity. Location of tax preparation booths in busy retail outlets or in the lobby of a car dealership or check casher can expose taxpayers to insecure handling of personal information.

In most states, there are no licensing requirements to become a tax preparer and no supervision of tax preparers by the IRS. The federal government regulates return preparers very minimally. Only three states (California, Maryland, and Oregon) license preparers; elsewhere, anybody can handle consumers' tax and financial information to prepare returns. This includes used car lots, electronics salesmen, financial service outlets, and furniture stores along with the established tax preparation firms. The IRS's National Taxpayer Advocate reported to Congress concerns about the privacy of tax returns held by the growing number of retailers and car dealers who make RALs to the working poor in anticipation of using the loan proceeds to make down payments on furniture, appliances, and used cars.

Storage and disposal of tax return information also are opportunities for identity theft or insecure handling of personal information, including failing to use password protected computers, locked files, and failing to shred documents no longer needed and return information to the taxpayer.

Pinero v. Jackson Hewitt Tax Services[94] was a class action lawsuit filed on behalf of over 100 Louisiana consumers whose tax returns and other financial documents were thrown in a public dumpster by Jackson Hewitt employees. These documents contained sensitive, confidential information, but were not shredded or otherwise destroyed before being placed in the dumpster. Plaintiffs alleged that the Jackson Hewitt franchisee's disposal of their records violated Section

[93] Beth McConnell, Public Interest Research Groups, "A Survey of Consumer Privacy Safeguards at Tax Preparation Booths," March 5, 2004.
[94] First Amended Complaint, Pinero v. Jackson Hewitt Tax Service, Civ. Ac. No. 08-03535 (E.D. La. July 15, 2008).

6103 of the IRS Code, the Federal Trade Commission's Disposal rule, the Louisiana Security Breach Statute, and Louisiana consumer protection law.

One of the 656 data breach incidents for 2008 compiled by the Identity Theft Resource Center involved a tax service office in Washington whose office computers were stolen and offered for sale on Craig's List. Clients were warned of the risk of identity theft.[95] Another breach involved a Queens, NY, tax preparer who was charged with preparing false state tax returns using Social Security numbers and credit card information from dozens of tax return clients. The tax preparer attempted to collect $4 million in fraudulent state tax refunds.[96]

H&R Block notified the Maryland Attorney General that a software error permitted some H&R Block Online message board users to have access to other users' correspondence with their tax preparers, in some cases including sensitive personal information. The company notified clients and provided a year of credit monitoring services.[97]

The Internal Revenue Service also abuses taxpayer privacy through its Debt Indicator program. The IRS screen reviews taxpayers for student loan debts, child support arrears, and other liabilities to the federal government that could reduce tax refunds, and shares that information with banks who are considering extending RALs to those clients. It is unclear whether taxpayers realize that the IRS operates a debt indicator program or that they are allowing the IRS to provide sensitive personal information to tax preparers about debts owed to the federal government.[98] The National Consumer Law Center (NCLC) reported that the IRS may be violating its own privacy law in providing the debt indicator service to tax preparers. IRS Form 8453 includes consent information in tiny print inadequate to clearly inform taxpayers that they are permitting the IRS to disclose whether they owe child support or student loan debt.[99]

Data Security Concerns with Remote Tax Preparation through Fringe Providers

Some fringe preparers operate by sending their customers' information to offsite tax preparers. TaxOne is a remote location tax preparation service provided by H&R Block to payday lenders, check cashers and other fringe financial outlets. Customers complete a Tax Information Organizer questionnaire at the partner outlet, and are instructed to bring their IRS Form W-2s, Form 1099s, a government issued photo ID, Social Security cards for all family members, and other requisite tax documents. The information is transmitted to TaxOne for preparation. Consumers return to the outlet to review the completed tax return and decide on "which fast money option works best for you."

TaxOne allows the fringe financial outlet to promote refund anticipation loans. TaxOne RALs are made by Santa Barbara Bank & Trust and BanComer. The RAL prices appear to be similar to H&R Block's in-store prices.[100] While the RALs may be less expensive than other providers'

[95] ITRC Breach ID 20080819-02, Kingston Tax Service, Identity Theft Resource Center 2008 Breach List, page 66.
[96] ITRC Breach ID 20080324-05, Queens tax preparer, Identity Theft Resource Center 2008 Breach List, page 153.
[97] Letter from H&R Block Corporate Counsel to Maryland Attorney General, June 4, 2008. On file with CFA.
[98] Chi Chi Wu, "Corporate Welfare for the RAL Industry: The Debt Indicator, IRS Subsidy, and Tax Fraud," National Consumer Law Center (NCLC), June 2005. CFA joined with NCLC in requesting the IRS to terminate the debt indicator program.
[99] *Ibid.* p. 9-10,
[100] For example, taxpayers are charged a $30.95 account set-up fee plus a $28 finance charge for a $2,700 RAL, which is similar to Block's fees. http://www.taxone.com/fast_money_options.aspx, viewed February 10, 2009.

and the quality of tax preparation better than at other payday lenders, the downside is that TaxOne allows payday loan chains to keep their customers coming through the doors during a time of year when typically the demand for payday loans drops. Some of the payday lenders and fringe financial providers using TaxOne include Check into Cash, MoneyTree, Advance America, Allied Cash Advance, and U.S. Money Shops. [101]

In addition, using a remote service to prepare tax returns and sell RALs or Refund Anticipation Checks (RACs) raises privacy and security issues, as sensitive information is passed back and forth between two or more entities. Payday lenders using TaxOne will complete a taxpayer's worksheets and documents, then scan and transmit them to the H&R Block staff to prepare the tax returns. TaxOne's website says that paper copies of tax information are returned to the taxpayer and not kept at the fringe financial outlet.

Both a privacy and a security policy are posted for TaxOne.[102] However, the consent forms required under Section 7216 of the IRS code are not initially handed out along with the TaxOne Organizer at storefront outlets or posted on the TaxOne website. The H&R Block training materials for TaxOne state that clients are to be provided the IRS-required consent-to-disclose forms to sign in order to permit their personal information to be shared with TaxOne for tax preparation purposes. Outlets are also required to provide consent-to-use forms for customers to authorize tax return information to be used to provide RALs.[103] It is not clear that the required notices are provided in timely fashion as required by IRS regulation.

Another remote tax preparation company, Liquid Tax, offers its remote tax preparation services to rent-to-own stores, check cashers, used car lots, barber shops, convenience stores, beauty supply shops, pawn shops and outlets that sell prepaid telephone cards. Taxpayer documents are faxed to Liquid Tax's office in Atlanta and the RAL checks are printed at storefront retailers who "convert loyal customers into additional revenues by providing basic tax prep services." Dealers are promised up to $100 in commission per return.[104]

Liquid Tax uses Drake Software to process tax returns and sell RALs.[105] Taxpayers fill out a form that the brick and mortar store faxes to the staff at Liquid Tax. The completed tax return and refund confirmation is faxed back within a half hour. A description of this product at the rent-to-own industry's trade website says that the client returns the next day to "pick up his refund check that is printed on the spot."[106] Of course, the check is for the proceeds of a RAL since IRS refunds are not processed in 24 hours.

Other tax preparation companies also advertise remote preparation services to check cashers and payday lenders. For example, Ultimate Tax Service offers check cashers a way to increase revenue by charging to prepare returns, then charging to cash the checks. Information is entered

---

[101] www.taxone.com/find_locations.aspx, viewed January 28, 2009.
[102] http://www.taxone.com/faq.aspx, viewed February 10, 2009.
[103] Email from H&R Block, TaxOne Training Document excerpt, February 1, 2009, on file with author.
[104] Press Release, "Liquid Tax's Powerful, Speedy Solution Converts Loyal Customers into Additional Profits," PRWeb.com, October 15, 2008, available at http://www.prweb.com/printer/1471614.htm, viewed February 10, 2009
[105] "Strong Partners: Liquid Tax Grows its Practice Through Unique Partnerships," Taxing Subjects, at http://www.taxingsubjects.com/Archives/issue24/art2.html, viewed February 10, 2009.
[106] "Dave Oliver Adds Liquid Tax to First American Home Furnishings Lineup," RTOonline.com, December 8, 2008.

"into the system," the remote preparer completes the return, and "you print the Refund Loan Checks in your office."[107]

Tax Preparation/Refund Anticipation Loan Privacy Enforcement Cases

Tax preparers sell several financial service products along with tax preparation, based on sharing tax return information with third party banks or providers. Refund anticipation loans, refund anticipation checks and audit insurance are commonly sold along with tax preparation services. The sale of financial products and services based on information in the consumer's tax return has led to litigation by state Attorneys General.

The California Attorney General filed lawsuits against all three major tax preparation chains in 2006-2008. The lawsuits alleged that these companies made misleading statements in their promotion of RALs and RACs, and violated consumer protection laws in their cross-lender debt collection practices. The lawsuits also alleged that the tax preparation chains violated IRS privacy rules regarding sharing of tax return information for cross-marketing.[108]

In December 2008, H&R Block agreed to enter into a settlement with the Attorney General, promising reforms of its practices and paying $2.45 million in consumer refunds plus $2.4 million in penalties and costs.[109] In addition, H&R Block agreed to cease any deceptive or misleading marketing of RALs, and to make clear and conspicuous disclosures to consumers prior to their purchase of a RAL or RAC. The lawsuit against Jackson Hewitt had been settled in 2007.[110]

RALs Facilitate ID Theft[111]

RALs are the tool of choice for fraudsters who commit tax identity theft. In March 2008, a *Wall Street Journal* article about the growing problem of tax ID theft featured several cases in which RALs were used to perpetrate that crime.[112] The NCLC/CFA comments in the IRS rulemaking included several stories about taxpayers who were victimized by tax ID theft perpetrated using RALs.[113]

In 2007, a Senate Finance Committee hearing on tax fraud and ID theft featured the testimony of Evangelos Dimitros Soukas, who netted over $40,000 by stealing the identities of other taxpayers as well as making up false returns. Mr. Soukas was initially attracted to the crime of

---

[107] Ultimate Tax Service ad, ChekList, Winter 2008, at 23.
[108] Complaint, California v. JTH Tax, Inc., Case No. CGC-07-460778 (Cal. Super. Ct. Feb. 26, 2007); Judgment, People of the State of California v. Jackson Hewitt, Case No. 070304558 (Cal. Sup. Ct. Jan. 3, 2007); People of California v. H&R Block, 2006 WL 2669045 (N.D. Cal. Sep. 18, 2006).
[109] Judgment, People of the State of California v. H&R Block, Case No. 06-449461 (Cal. Sup. Ct. Dec. 31, 2008)
[110] Judgment, People of the State of California v. Jackson Hewitt, Case No. 070304558 (Cal. Sup. Ct. Jan. 3, 2007)
[111] For a full report on the impact of RALs on fraudulent tax filing, see: Chi Chi Wu and Jean Ann Fox, "Big Business, Big Bucks: Quickie Tax Loans Generate Profits for Banks and Tax Preparers While Putting Low-Income Taxpayers at Risk," Appendix A: RALs, Tax Fraud, and Fringe Preparers. National Consumer Law Center and Consumer Federation of America, February 2009. http://www.consumerfed.org/pdfs/2009_RAL_Report.pdf
[112] Tom Herman, "Identity Thieves Target Tax Refunds," *Wall Street Journal*, March 12, 2008.
[113] Appendix D to NCLC/CFA Comment to IRS RAL ANPR.

tax identity theft and tax fraud because of a RAL website advertisement, and used RALs in his criminal schemes.[114]

IRS Rules for Privacy and Security of Tax Return Information

IRS Code Section 7216 provides criminal sanctions when any person "engaged in the business of preparing, or providing services in connection with" income tax return preparation either knowingly or recklessly discloses any information furnished for preparation of tax returns or uses this information for any purpose other than return preparation. The National Taxpayer Advocate told the American Bar Association in 2006 that "the protection of taxpayer information by the IRS and preparers is an absolute necessity for maintaining taxpayers' confidence and their willingness to uphold their end of the social contract." The Taxpayer Advocate stated that taxpayer consent to use or disclose tax return information should be narrowed to only those purposes that are tax-related, which does not include disclosing information to a bank to obtain a refund anticipation loan or an Individual Retirement account.[115]

Congress gave the IRS the power to issue regulations making exceptions to that prohibition on secondary use of tax return information. The IRS proposed changes to its rules implementing Section 7216 of the Internal Revenue Code to improve consent forms signed by taxpayers to permit sharing and use of tax return information. Consumer organizations and state Attorneys General filed comments urging more stringent privacy protections.[116]

The consumer groups called for a ban on the use and sharing of tax return information for purposes other than preparing and filing tax returns with the IRS, citing the risk of security breaches, ID theft, and aggressive marketing of products and services based on taxpayer returns. The groups argued that the threats posed by tax preparation companies using or sharing detailed tax-related financial information, such as income, investments, and dependents, for any purposes other than tax return filings far outweighed the protection of the rule's consumer consent requirement.

However, the IRS rejected recommendations by consumer groups and by the majority of state Attorneys General to prohibit tax preparers from trafficking in tax return information for cross-marketing purposes and expanded the "gaping loopholes" that already allow sharing and marketing based on tax records. The new privacy rule which took effect January 1, 2009, places the burden of protecting sensitive tax return information on taxpayers instead of prohibiting preparers from sharing tax return information for marketing purposes. The IRS now permits tax returns to be sold, shared, or used by both tax preparers' affiliates and third party companies as long as taxpayers sign a consent form. Once tax return information has been shared with third-parties, it is not subject even to modest existing IRS protections and falls under weaker nontax privacy laws.

---

[114] Statement of Evangelos Dimitros Soukas, *Testimony before the Senate Finance Committee*, April 12, 2007.
[115] Nina Olson, National Taxpayer Advocate, Keynote Address, American Bar Association Tax Section, May 5, 2006. See, also Dustin Stamper, "Olson Calls for Outlawing All Taxpayer Data Disclosures for Nontax Purposes," Tax Analysts, May 8, 2006.
[116] Comments of National Consumer Law Center, Consumer Federation of America, and US PIRG, regarding Notice of Proposed Rulemaking Amendments to Section 7216 Regulations and Revenue Guidance, 26 CFR Par 301, RIN-1545-BA96, March 2005, http://www.consumerfed.org/pdfs/IRS_Privacy_Rule_Comments.pdf .

The IRS privacy rule expanded permission for sharing and use of tax return information to third-party companies as well as affiliate entities as long as preparers get signed consent, either on paper or through electronic signatures. The rules that took effect in January 2009 made some improvements in consent procedures and required affirmative consent for preparers to ship returns outside the United States.

Advocates warned that any consent form will end up as another document in the stack of papers thrust upon taxpayers during the tax preparation session. Taxpayers told to 'just sign here and here' by their tax preparers may unknowingly consent to giving up their most sensitive financial information to marketers.

At the same time that the IRS issued its weak final privacy rule, the IRS asked for comments on developing rules restricting the sharing of tax return information specifically to market refund anticipation loans, refund checks, audit insurance and other high cost products typically sold to low income taxpayers. Although NCLC and CFA filed extensive comments in that IRS docket[117], no changes have been made to the tax return privacy rules. Instead, the IRS Commissioner announced a series of public forums in 2009 to gather suggestions on how to improve tax preparation. CFA spoke at the IRS Forum in July 2009 and filed comments jointly with NCLC recommending that the IRS amend its 7216 regulations to prohibit the sharing and/or use of tax return information for purposes of selling or arranging financial products. We also recommended that the IRS stop providing the debt indicator service to tax preparers and their partner banks.[118]

Conclusions

Consumer financial and personal information is inadequately protected by federal privacy laws, by supervision of non-bank financial service firms, or by specific rules that govern access to consumers' bank accounts or the sharing and secondary use of tax returns. Despite lengthy privacy policies and boilerplate security promises, consumer financial information is easily used for purposes other than the original transaction. Companies do not have to obtain consumer consent to share and use personal information except in the case of tax preparers sharing tax returns. And, even then, once a tax return has been shared with a marketer or bank, that entity does not have to get affirmative consent to reuse consumer information.

Consumers are at risk of identity theft and security breaches due to unsafe handling of personal financial information held by non-bank financial service companies. Consumers are exposed to targeted marketing based on information shared by financial service providers. The design of payday loans, and the scant or lax regulation of lenders that hold consumers' personal checks or have electronic access to bank accounts as security for loans, exposes borrowers to bank account risks such as unauthorized debits, repeat deductions from accounts, and coercive collection

[117] Comments of National Consumer Law Center, Consumer Federation of America, et al. regarding Advance Notice of Proposed Rulemaking – Guidance Regarding Marketing of Refund Anticipation Loans (RALs) and Certain Other Products, April 7, 2008, available at http://www.consumerlaw.org/issues/refund_anticipation/content/comments_040708.pdf.

[118] Jean Ann Fox and Chi Chi Wu, "IRS Commissioner's Return Preparer Review Forum Comments," IRS Notice 2009-60, August 12, 2009. http://www.consumerfed.org/pdfs/CFA_and_NCLC_comments_on_RALs_to_IRS_8-12-09.pdf.

tactics. Failure to adequately screen loan applications against bank account ownership results in payday loans taken in consumers' name by ID thieves.

The bottom line is that Fair Information Practices should be the rule, not the exception. These principles provide for limited information collection, data quality standards, specification for the use of information, limits on use, security safeguards, and accountability. Financial service providers should have to obtain consumer consent to use personal financial information for secondary purposes. Privacy policies should insure privacy, not spell out all the ways consumers have little or no control over the many ways their information is shared and used.

Congress should ban lending secured by holding a borrower's unfunded check or single electronic debit or demand draft. The IRS or Congress should stop tax preparers from sharing, using or selling tax return information for commercial purposes.

Appendix A

FTC ID Theft and Credit Complaint Survey

CFA filed a Freedom of Information Act request with the Federal Trade Commission in 2007 to collect a small sample of complaints filed by consumers with the ID Theft Center and complaints filed alleging violations of the Gramm-Leach-Bliley Act's security and privacy requirements. Since the Federal Trade Commission is the only federal agency that enforces consumer privacy and security laws and regulations with respect to non-bank financial service providers, CFA sought to learn about the types of complaints consumers file against fringe financial service providers.

Sixty-six ID Theft cases reported to the FTC on September 20th and 21st, 2007 were provided in redacted form. These were complaints as filed but not investigated. The complaint intake forms briefly described the complaint, sometimes noted the dollar amount of harm, and noted whether the consumer had reported the theft to either law enforcement or the credit reporting agencies. Victims of identity theft reported a variety of unauthorized financial transactions initiated using stolen identities, ranging from mortgages, credit cards, auto loans and leases, bank accounts, Sallie Mae student loans, and small loans. Consumers reported debt collection contact; being subject to civil lawsuits; experiencing employment fraud, utility accounts opened in the victim's name, and government benefits obtained using the victim's Social Security number, name, address, and/or date of birth.

In most cases, the intake forms note that inadequate security procedures were the basis for the complaints. Frequently, the ID theft victim did not know the perpetrator or how the information was obtained. Family members or employers with access to personal information were implicated in some cases. In one case the victim named a Girl Scout troop as the source of the ID theft. Consumers learned about the theft through entries on credit reports, calls by debt collectors, or being turned down on credit applications.

Eight of the 66 ID theft reports involved credit obtained from fringe financial providers described in this paper.

Two consumers reported that online payday loans from a large online lender in the US had been obtained using their information. In one case the incident also involved new bank accounts opened in the consumer's name and denial of credit due to nonpayment of the unauthorized loans. A second consumer reported $2,500 in online payday loans from the same company in the victim's name. This incident was also reported to police in San Antonio, Texas.

Three additional online payday loans were allegedly made to people using stolen identities. One consumer reported $1,400 in loans obtained in her name from three online lenders and debt collection threats of a lawsuit for nonpayment. Another complaint was filed about online payday loans taken out by an Arizona person using the victim's Social Security number. Over the time period March 7, 2007 through September 7, 2007, thirteen loans were made to the ID thief. When the borrower failed to pay the last loan, the company ran a check on the SSN and discovered it was the complainant's. Quickestcashadvance.com gave an online payday loan worth $450 to a family member, using the ID theft victim's information.

A consumer reported debt collection effort on an unauthorized payday loan from a retail payday loan outlet at a cost of $587. The consumer reported being told that the fraudulent applicant used the consumer's name and Social Security number but a different date of birth on the original application.

Two consumers called the FTC to report fraudulent tax filing and/or refund anticipation loans. In one case, the consumer reported $6,313 in unauthorized loans. The second consumer reported $3,290 in an unauthorized refund anticipation loan and fraudulent income tax return filed.

CFA also requested a sample of complaints regarding credit issues filed with the Federal Trade Commission. We received 190 credit complaints filed on September 21, 2007, covering problems involving the Federal Trade Commission Act, Telemarketing Sales Rule, Gramm-Leach-Bliley Act and other credit related issues. Of the total complaints in this sample, twenty-four involved high cost small loans. Details of complaints are listed below. Note that these are complaints as filed, not investigated by the FTC.

Six complaints were filed against a California small loan company that marketed its loans nationwide via the internet. One complaint reported that after the first payment, the interest rate went up for no reason. After making four payments, she found out that payments were applied to the interest. [119] A second complaint involved a loan for $2,525 at 99.25% APR. The complaint alleged that the loan company made an unauthorized withdrawal from his checking account by not honoring an agreed to payment extension.[120] Other complaints noted changes in the due date, triggering a $15 late fee; high principal after a year of payments for a loan costing 59 percent interest rate; a balance that increased despite making monthly installments; and repeated marketing phone calls at the consumer's place of employment.[121]

Other complaints filed with the Federal Trade Commission on credit and privacy issues named online payday lenders and reported unauthorized withdrawal from a bank account, debt collection harassment and threats, continuous withdrawals from the borrower's account (borrowed $200, $800 taken from account); difficulty stopping repeated withdrawals of finance charges without paying down the debt; mix-up of loan proceeds deposited into a closed account and threats of fraud; online payday loan made using ID theft victim's Social Security Number; unauthorized $49.95 withdrawal from an account although incomplete online payday loan application; repeat withdrawals by an online payday loan company other than the one to which the consumer applied/no contract or contact information; undelivered loan from online payday loan referral company; repeat presentment of debit which triggered insufficient funds fees from both bank and payday lender, legal threats and faxed information to employer; large line of credit provided instead of small payday loan applied for, and difficulty terminating transaction to prevent withdrawal of funds.[122] In another complaint, the consumer stated that her information was provided to an online payday lender but no loan was made. A consumer reported that despite not applying for an online payday loan, funds were placed in his bank account then immediately withdrawn. Subsequently the online lender withdrew another $470 from the

[119] FTC Ref. No. 11612507
[120] FTC Ref. No. 11612533
[121] FTC Ref. No. 11641914. 11651901. 11632839, 11625380.
[122] FTC Ref. No. 11613163, 11613174, 11623928, 11625987, 11631983, 11632031, 11633577, 11649373, 11650442, 11623332, 11624504,

consumer's account, triggering overdraft fees and the consumer having to close the account to stop continued withdrawals. The consumer was referred to the FTC by the bank. In another case, the borrower reported that withdrawals from the bank account more than repaid the online payday loan. The consumer filed fraud charges at his bank but the bank could not stop the electronic withdrawals. Another consumer complained that a scheduled online payment was made at a later date than expected, triggering an overdraft.[123]

Consumers also filed complaints with the FTC about car title loans. In one case, the consumer alleged that a loan was given to a consumer secured by a car not registered to that person. A South Carolina consumer complained about collection arrest threats after making three payments of a $600 loan before losing her job.[124]

[123] FTC Ref. No. 11631527, 11631430, 11631117, 11631024, 11626059
[124] FTC Ref. No. 11632523, 11624886