



2004 Summit on Protecting Teens from Identity Theft

Key Findings

November 16, 2004

Table of Contents

The Challenge	1
Qwest's Commitment	2
2004 Summit	3
Summit Panel Findings & Recommendations	4
Preventing Identity Theft	5
Appendix	
Qwest Consumer Protection Program Overview	9
Additional Resources	11
Summit Panel of Experts	12

The Challenge

Defining the Issue – Identity Theft of Teens

Nearly five years after Congress passed the 1998 Identity Theft Act, the Federal Trade Commission (FTC) made a startling discovery: The problem of “stealing” another person’s personal identifying information was considerably more widespread and pernicious than previously realized.

According to the FTC’s, 2004 survey “National and State Trends in Fraud and Identity Theft” revealed that nearly 10 million people – 4.6 percent of the adult population – had discovered that they were victims of some form of identity theft. Identity theft is a crime in which an imposter obtains key pieces of information such as Social Security and driver’s license numbers to obtain credit, merchandise and services in the name of his or her victim. The victim is left with a ruined credit history and the time-consuming and complicated task of regaining financial health.

The FTC survey also revealed identity thefts translated to some \$48 billion in losses to businesses, nearly \$5 billion in losses to victims, and approximately 300 million hours spent by victims attempting to resolve the problem.

The survey results prompted the FTC to significantly step up its consumer education campaign about identity theft as well as its support for law enforcement agencies prosecuting identity thieves. The commission’s Web site, **www.consumer.gov/idtheft**, now provides a wealth of information and resources for victims, law enforcement agencies and others interested in identity theft.

The revelation that identity theft is a widespread and growing problem caught the attention of consumer groups, local and state law enforcement agencies and the media. But generally overlooked in the ensuing publicity was an intriguing piece of demographic information contained in the 2003 survey: Young people in the 18-to-29 age group are the number one target for identity thieves, comprising 31 percent of the total thefts.

With little or no knowledge of financial transactions or credit reports, teenagers and young people are particularly vulnerable to identity theft. Identity thefts can occur before a teenager even reaches the age of 18, the time when most minors are eligible to enter into contracts and apply for credit cards. Many teenagers discover they are a victim of identity theft when they first apply for a driver’s license and find that one has already been issued to someone else under the same Social Security number.

Because teens are less educated about identity theft, they tend to be more susceptible to the dangers of the crime. For this reason, Qwest Communications believes in the importance of educating our nation’s youth so that they become empowered to take the necessary steps to reduce the incidence of identity theft.

Qwest's Commitment

Building Awareness – Identity Theft of Teens

Today's teens are increasingly technology savvy. In fact:

- 56 percent of all teens own or use a wireless phone (Yankee Group, 2003 Mobile User Survey)
- 82 percent of young people own or use a computer (Born To Be Wired Yahoo! Carat Interactive Research 2003)
- On average, teens spend more than 16 hours on the internet per week (Born To Be Wired Yahoo! Carat Interactive Research 2003)

According to David Heller, Qwest vice president of risk management and chief compliance officer, teens comprise approximately 20 percent of Qwest's customer base.

“Qwest recognizes that while there are nationwide efforts in place to reduce the incidence of and raise awareness for identity theft, teens are being overlooked as a key audience,” said Heller. “With the right information disseminated to teens before they receive their first driver's license, checking account or credit card, Qwest believes teens can learn how to protect themselves from identity thieves.”

Because teenagers are not the typical audience of various identity theft education efforts, Qwest has inaugurated a comprehensive teen education and awareness program tailored specifically to their age group. Teen education is part of Qwest's overall Consumer Protection Program (see page 9 for more information).

Recognizing the need to build awareness and understanding, Qwest launched its teen education initiative by hosting a landmark summit to shed light on this critical issue for the first time.

Other key components of Qwest's teen education program include:

- Information Portal designed specifically for teens and located at www.highwayqwest.com/identitytheft.
- Teen Video (free and available for download at www.highwayqwest.com/identitytheft) that educates teens about the danger of fraud and identity theft, how to prevent it, and what to do if their identity is stolen.

Qwest's *2004 Summit on Protecting Teens from Identity Theft* convened in Denver on Oct. 20, 2004.

2004 Summit on Protecting Teens from Identity Theft

Summary of Key Findings

For the first time, influential members from business, government, law enforcement, education and civic groups joined forces with an expert panel in Denver at Qwest's *2004 Summit on Protecting Teens from Identity Theft*. The Summit's goal was to build awareness for this issue and to develop initiatives to help protect teens from identity theft.

The panel of experts (see pages 12-14 for bios) included:

- Linda Foley, co-executive director, Identity Theft Resource Center
- Jay Foley, co-executive director, Identity Theft Resource Center
- Rhea Takara, identity theft victim
- Betsy Broder, assistant director, Federal Trade Commission's Division of Planning and Information
- Diane Terry, senior director of fraud victim assistance department, TransUnion
- Jeff Tricoli, special agent, FBI Denver Division
- David Rakow, prosecutor, Rockwall County, TX
- Melodi Mosley Gates, director of information security, Qwest Communications
- Kent Prose, senior criminal investigator, Denver District Attorney's Office

The first half of the Summit leveraged the panel's expertise to build awareness for the issue of the identity theft of teens. Representing key areas on the issue's spectrum – consumer interest groups, federal government, credit reporting agencies, businesses, law enforcement and teen victims – the Summit's panel identified the following significant findings:

- Public and private entities need to create and develop partnerships to extend the reach of this message – protecting teens from identity theft.
- Both high schools and colleges need to integrate identity theft awareness and prevention into their curriculums.
- Law enforcement and government agencies must work together and stay attuned to developments in technology and tools in the private sector developed to spot fraud.
- Institutions with sensitive personal information – especially business and schools – need to establish better controls and practices to ensure identities remain safe.

A detailed overview of the expert panel's recommendations can be found on pages 4-5. Recommendations were made in the following areas: building teen awareness, school involvement, prosecuting identity theft and the role of business.

The second half of the Summit was devoted toward generating ideas for ways in which teens can protect themselves from identity theft. Because teens have not been previously targeted for education on this issue, Summit participants developed a unique list of prevention tips for teens and parents, as well as for general consumers. These tips can be found on pages 6-7.

Summit Panel Findings & Recommendations

Building Teen Awareness

- Identity theft affects teens in the same way it affects adults. Identity thieves don't discriminate by age, gender or race.
- Teens are easy targets of identity theft because they are less educated about the crime, its prevention and warning signs that suggest they may be victims.
- Teens are currently spending more time on the internet than are adults and tend to be more careless about sharing their personal information online – which is where most identity theft schemes occur. And, teens are less likely to check their credit than are adults.
- We need to find ways to reach as many teens as possible with focused education that teaches them to handle their personal information wisely.
- It's essential to continue to create partnerships between public and private entities to extend the reach of this message. Using and expanding these partnerships will help us to reach as large an audience as possible.

School Involvement

- The classroom is an ideal place to educate teens before they become the primary targets of identity theft. High schools and colleges need to integrate identity theft awareness and prevention into their curriculums.
- Many of today's schools utilize computer technology in the classroom learning environment. Students need to be taught safe usage of computer technology, including password protection, avoiding "phishing" e-mails and e-mails containing viruses, and not storing personal information on devices such as laptops, wireless phones, pagers and MP3 players.
- Colleges and universities need to help protect teens and young adults from identity thieves. For example, these institutions should stop publicly displaying the Social Security number in any situation and discontinue using it as a student identification number.
- College students should have access to cross-cut shredders and as well as locked containers to store personal and financial information as well as technology such as laptops, wireless phones, pagers and mp3 players.

Prosecuting Identity Theft

- Because teens are seldom aware of warning signs suggesting identity theft, there is usually a long delay before they realize they've become victims. In many cases involving teens, the identity thieves are family members or friends.
- State statutes need to be worded more precisely to protect teens because it's extremely difficult to get teen victims to follow through with filing criminal complaints.
- Law enforcement and government agencies must continue to work together and stay attuned to developments in technology and tools in the private sector developed to spot fraud. These same groups must keep a vigilant eye on the newest scams intended to separate consumers from their good name.
- As technology and society advance, so does the complexity of methods in which individuals steal identities. Identity thieves are increasingly resourceful and are using technology in creative ways to trick people into

divulging personal information. Phishing, spoofing and other online trickery are just a few of the ways that high-tech criminals are getting at personal and financial information.

- There is a lack of funds and insufficient manpower to prosecute the many emerging variations of identity theft in a timely manner.
- Correlations exist between drug-related crimes and identity theft. For example, many methamphetamine addicts use identity theft as a way to support their drug habits.
- There is also a growth in identity theft originating from countries outside the United States as well as organized crime operations within the country.

The Role of Business

- Because today's teens are the most active users of technology, they represent a large and important market segment. As laptops, wireless phones, pagers, MP3 players and other technology devices become commonplace for teens, so does the risk of identity theft.
- Businesses marketing products that store personal information need to educate teens and all consumers about the ways in which they can protect their identities while using these products.
- Recovering from identity theft crimes is a major expenditure for businesses – in both time and money. All businesses – not just financial institutions – need to take reasonable precautions to protect their own employees and customers from identity theft.
- Businesses should conduct a thorough review of how they acquire, distribute, store and dispose of sensitive personal information. Business need to ask themselves some questions about identity theft. For example:
 - Do we really need the information we're asking for – such as Social Security numbers – and, if so, are we acquiring it in a safe manner?
 - What computer security measures have we placed around the systems storing data?
 - Who has access to sensitive information from employees and customers and have they gone through a background check?
 - Are documents containing personal information shredded or rendered unreadable before disposal in office trash containers and company dumpsters?
 - Do we provide our employees with a secure place to store their purses, wallets and laptops containing personal information?

Preventing Identity Theft

Tips for Teens, Parents and General Consumers

5 Tips for Teens to Prevent Identity Theft

1. ***Don't be intimidated.*** Tell adults (e.g. coaches, teachers and employers) who ask for Social Security, driver's license and credit card numbers that you want to know how they'll use it and how they'll protect it from identity theft.
2. ***Guard your personal information.*** It's valuable, so password-protect your laptops, wireless phones, pagers and MP3 players and don't store personal identification information on these and other devices. Carefully destroy papers you throw out – using a cross-cut shredder if possible – that contain personal identifying information.

3. ***Check yourself out.*** When you turn 16, frequently check bank and credit card statements for irregularities and ask for help on how to monitor your credit reports at least once a year.
4. ***It's OK to say "NO."*** Don't loan out any form of personal identification such as a driver's license or passport, even to a friend.
5. ***Protect your Social Security number.*** Even when asked, don't provide your Social Security number when applying for your first job. It's not necessary. Also, don't use your Social Security number on your driver's license.

5 Tips for Parents to Help Teens Prevent Identity Theft

1. ***Stay alert.*** Be on the lookout for unsolicited credit card offers in your teen's name. The only way teens can get these offers is if they have a credit history.
2. ***Monitor your teen's credit.*** Frequently check your teen's bank and credit card statements for irregularities.
3. ***Safely store personal identification information.*** Make sure your teen's Social Security card and passport are stored in secure locations. Your teen's wallet, school bag or car are not safe places.
4. ***Teach teens about technology scams.*** Educate your teen about the dangers of "phishing" e-mails, e-mails containing viruses and chat rooms.
5. ***Encourage password protection.*** Help your teen create effective passwords – a combination of numbers and letters only they will remember – for their laptops, wireless phones, pagers and MP3 players. Be sure they know how to password-protect these devices and that they're not storing personal information on them.

10 Tips for General Consumers to Prevent Identity Theft

1. Shred all documents that contain personal financial information before throwing them away.
2. Monitor your credit reports.
3. Review your credit card and bank statements monthly. Watch for unfamiliar transactions.
4. Do not print your Social Security number on your checks or driver's license.
5. Save your receipts and take all credit card and ATM receipts with you after you pay for goods or services.
6. Opt out of unsolicited credit card offers. Call 888-567-8688.
7. Do not send mail from an unsecured mailbox. Identity thieves often try to steal your outgoing mail.
8. Maintain a list of phone numbers with the contact information of your credit card, bank and other financial institutions. If a credit card is lost or stolen, contact the company immediately.
9. When online, never provide financial information unless you initiate the transaction. Do not respond to any e-mail that requests personal and financial information.
10. For additional and detailed information, visit www.qwest.com/identitytheft.

APPENDIX

Qwest Consumer Protection Program Overview

As part of Qwest's Spirit of Service, the company recently launched its Consumer Protection Program to help educate its customers and all consumers about the growing epidemic of identity theft crimes. This comprehensive program will help consumers of all ages learn about the dangers of fraud and identity theft, how to prevent it, and what to do if their identity is stolen.

The four key program components are:

- A partnership with the Denver District Attorney
- Teen education
- Information hub
- Community seminars

(1) Partnership with the Denver District Attorney

During the summer of 2004, Qwest joined forces with Denver's District Attorney's Office to create a fraud and identity theft video designed to educate consumers. The video, *Identity Theft - Don't Be a Victim*, highlights statistics about the escalating crime of identity theft. It also details the potential widespread and negative impact identity theft can have on its victims and offers proactive measures that consumers can take to reduce the risk of being victimized.

Qwest is distributing this video to businesses and community organizations throughout Qwest's 14-state region. For more information on obtaining the free video, visit www.qwest.com/identitytheft.

(2) Teen Education

Qwest hosted the 2004 Summit on Protecting Teens from Identity Theft on October 20, 2004, to address the increasing fraud and identity theft issues faced by teens. The Summit brought together influential members from business, government, academia and the media to identify the problems teens face with respect to identity theft and develop initiatives to help protect them.

In addition, Qwest has developed an informational Web site at www.highwayqwest.com/identitytheft for teens. At the site, teens can learn about:

- Common forms of fraud and identity theft
- How to prevent fraud and identity theft
- Warning signs that they've become a victim
- What to do if they've become a victim.

The Web site also includes a free downloadable video about identity theft and an online "calculator" that asks teens to fill out a short survey in exchange for a score representing their current level of fraud and identity theft risk and awareness.

(3) Information Web Site

Qwest created www.qwest.com/identitytheft -- a user-friendly resource where consumers can educate themselves about all aspects of identity theft.

This Web site serves as a comprehensive resource guide for consumers to learn how to protect themselves from identity theft. The site features an identity theft "calculator" to help consumers rate their level of knowledge about identity theft.

(4) Community Seminars

Beginning in 2005, Qwest will host a series of fraud and identity theft community seminars throughout Qwest's 14-state region.

Additional Resources

Comprehensive information can be found on the following Web sites:

- Qwest Communications – www.qwest.com/identitytheft
- Identity Theft Resource Center - www.idtheftcenter.org
- Federal Trade Commission - www.consumer.gov/idtheft
- TransUnion – www.transunion.com
- Federal Bureau of Investigation – www.ifccfbi.gov
- Privacy Rights Clearinghouse - www.privacyrights.org
- National Fraud Information Center - www.fraud.org
- Better Business Bureau – www.bbb.com
- National Consumers League – www.natlconsumersleague.org
- United States Secret Service – www.treas.gov.uss
- Social Security Administration – www.ssa.gov
- Fight Identity Theft – www.fightidentitytheft.com
- ScamBusters – www.scambusters.org
- Electronic Privacy Information Center – www.epic.org

Summit Panel of Experts

Linda Foley, co-executive director, Identity Theft Resource Center, San Diego, CA

A former victim of identity theft herself, Linda Foley co-founded the Identity Theft Resource Center (ITRC) in 1999 in response to the growing need for victim assistance and public empowerment due to the epidemic rise in identity theft crimes. A nationwide nonprofit identity theft program based in San Diego, Calif., ITRC supports thousands of victims through its Web site (www.idtheftcenter.org), e-mail and telephone correspondence.

Foley provides testimony and information for national and state conferences and taskforces, and is a resource for legislators throughout the nation. She has appeared on major television news and talk shows, and is widely quoted by major newspapers, radio stations and magazines. In addition to her community work, Foley advises corporations in the development of better document handling procedures. She has received numerous awards and recognitions, including the 2004 National Crime Victim Service Award presented by the U. S. Attorney General for the Department of Justice, and commendations by U.S. Senator Dianne Feinstein and former California Governor Gray Davis.

Jay Foley, co-executive director, Identity Theft Resource Center, San Diego, CA

As ITRC's primary criminal justice contact, Jay Foley has received great support and accolades from members of law enforcement across the country who frequently refer victims to him for assistance. Foley currently sits on law enforcement, governmental and legislative taskforces, including JAG, and he has testified at legislative hearings in various states and in front of Congress.

With more than 20 years of experience in project management and customer service training, Foley is also a popular presenter and trainer. His military experience and studies in computer science provide him a unique understanding of the computer's role in identity theft crimes.

Foley has appeared on many major television news programs and has been quoted by most major newspapers and radio stations across the country. He is also a recipient of the 2004 Crime Victims Service Award presented by the U. S. Attorney General for the Department of Justice, and commendations by Senator Dianne Feinstein and former California Governor Gray Davis.

Rhea Takara, identity theft victim, San Diego, CA

At the age of 24, college student Rhea Takara received a late notice for a credit card bill. Recognizing that this was not a credit card she had applied for or seen before, she immediately contacted the company to ask about the account. Through her extensive research, she discovered that her father had stolen her identity when she was 18 years old. Undetected for six years, he took out loans in her name and ruined her credit. Now 27, Takara has spent the past three years working to correct her father's wrongdoing and clear her name.

Betsy Broder, assistant director, Federal Trade Commission's Division of Planning and Information, Washington, D.C.

In her current role at the FTC, Betsy Broder helps coordinate the agency's collection and analysis of consumer-related data, including the critical database and information sharing functions for identity theft and consumer fraud. She also assists in the oversight of the FTC's other identity theft initiatives, including coordination with other law enforcement agencies, outreach to industry, and consumer education. In her 16 years at the FTC, Broder has supervised consumer fraud litigation in federal court and led the investigation and civil prosecution of telemarketing boiler rooms, Internet pyramid schemes, and business and franchise scams in courts throughout the United States. Previously, Broder was an Assistant Attorney General for the State of New York.

Diane Terry, senior director, TransUnion Fraud Victim Assistance Department, Corona, CA

Diane Terry is co-founder and senior director of the TransUnion Fraud Victim Assistance Department (FVAD). In this role, she is responsible for leading the FVAD's efforts in working with consumers, law enforcement and financial service industry professionals in combating and preventing the crimes of identity theft and credit fraud. During her more than 31 years with TransUnion, she has played an important role in numerous major fraud investigations; advised federal, state and local law enforcement agencies; taught courses on financial crimes; and written extensively on the subject of credit fraud and identity theft. She is an instructor for the Department of Justice economic crimes class and has been an active member of the International Association of Financial Crimes Investigators since 1981, where she currently serves as vice president.

David Rakow, chief felony prosecutor for the Criminal District Attorney's Office in Rockwall County, TX

During his long and distinguished career as a prosecuting attorney, David Rakow has prosecuted and convicted murderers, rapists, child molesters, drug dealers, family violence offenders, drunk drivers and thieves. He has recovered restitution for victims, provided protective orders for victims of domestic violence, aided drug addicts and the mentally ill in getting treatment, and removed children from abusive homes. Rakow has prosecuted identity theft cases, including that of a nine-year-old girl whose parents used her identity for criminal activity. He is an active member of the Texas District and County Attorney's Association.

Melodi Mosley Gates, senior director of information security & CISO, Qwest Communications, Inc., Denver, CO

With more than 18 years of information technology and telecommunications experience, Melodi Mosley Gates leads an organization with corporate-level Information Security (InfoSec) responsibilities for Qwest. Her key responsibilities include information security policymaking and standards development, compliance assurance and assessment activities, centralized identity management, monitoring for risks, vulnerabilities and managing cyber incidents, and protecting e-mail as it passes between Qwest and the internet. Her team also provides expertise and sales support for all Qwest business channels including a specialized team for government services security that supports the unique security needs of Qwest's federal customers.

Jeffrey A. Tricoli, special agent, Federal Bureau of Investigation, Denver, CO

Special Agent Jeffrey Tricoli has been with the FBI since 1998. In 2001, Tricoli worked for the National Infrastructure Protection Center (NIPC) located within the FBI Headquarters in Washington, DC. While working at the NIPC, he had the opportunity to testify before the Senate Select Committee on Intelligence and the National Security Council on threats to our nation's critical computer infrastructures. He is currently assigned to the Cyber Squad of the Denver FBI and is responsible for investigating computer intrusions, identity theft and crimes against children.

Kent Prose, senior criminal investigator, Denver District Attorney's Office Economic Crime Unit, Denver, CO

Since joining the Denver DA ECU in 2000, Prose has been the coordinating investigator on more than a dozen grand jury cases that involve identity theft. Those investigations have resulted in criminal cases against more than 175 defendants, including more than 20 convictions for violations of the Colorado Organized Crime Control Act (COCCA). Prose has team-taught classes regarding identity theft prosecution for the National White Collar Crime Center, the International Association of Financial Crimes Investigators, Colorado District Attorney's Council, Association of Certified Fraud Examiners, Colorado Adult Protective Services Supervisors, and other law enforcement and industry training programs.