

NOTICE OF MEETING AND AGENDA

**SPECIAL MEETING OF THE OPERATIONS OVERSIGHT COMMITTEE
and
BOARD OF RETIREMENT***

LOS ANGELES COUNTY EMPLOYEES RETIREMENT ASSOCIATION

**300 NORTH LAKE AVENUE, SUITE 810
PASADENA, CA 91101**

THURSDAY, NOVEMBER 9, 2017 - 9:00 A.M.**

*The Committee may take action on any item on the agenda,
and agenda items may be taken out of order.*

COMMITTEE MEMBERS:

Alan Bernstein, Chair
Anthony Bravo, Vice Chair
Joseph Kelly
Ronald Okum
David Muir, Alternate

I. APPROVAL OF THE MINUTES

A. Approval of the minutes of the special meeting of October 12, 2017

II. PUBLIC COMMENT

III. ACTION ITEMS

A. Recommendation as submitted by James Beasley, Administrative Services Analyst III: That the Committee recommend the Board of Retirement approve the purchase of Cyber Liability Insurance with North American Specialty (NAS) Insurance. (Memorandum dated October 23, 2017)

IV. FOR INFORMATION

A. LACERA Operations Briefing
JJ Popowich/Bernie Buenaflor

B. Overpayment & Forgery Receivables (Period Ended June 30, 2017)
David Bayha

November 9, 2017

Page 2

V. REPORT ON STAFF ACTION ITEMS

VI. GOOD OF THE ORDER

(For information purposes only)

VII. ADJOURNMENT

***The Board of Retirement has adopted a policy permitting any member of the Board to attend a standing committee meeting open to the public. In the event five or more members of the Board of Retirement (including members appointed to the Committee) are in attendance, the meeting shall constitute a joint meeting of the Committee and the Board of Retirement. Members of the Board of Retirement who are not members of the Committee may attend and participate in a meeting of a Board Committee but may not vote on any matter discussed at the meeting. The only action the Committee may take at the meeting is approval of a recommendation to take further action at a subsequent meeting of the Board.**

****Although the meeting is scheduled for 9:00 a.m., it can start anytime thereafter, depending on the length of the Board of Retirement meeting preceding it. Please be on call.**

Any documents subject to public disclosure that relate to an agenda item for an open session of the Committee, that are distributed to members of the Committee less than 72 hours prior to the meeting, will be available for public inspection at the time they are distributed to a majority of the Committee, at LACERA's offices at 300 North Lake Avenue, Suite 820, Pasadena, California during normal business hours from 9:00 a.m. to 5:00 p.m. Monday through Friday.

Persons requiring an alternative format of this agenda pursuant to Section 202 of the Americans with Disabilities Act of 1990 may request one by calling Cynthia Guider at (626)-564-6000, from 8:30 a.m. to 5:00 p.m. Monday through Friday, but no later than 48 hours prior to the time the meeting is to commence. Assistive Listening Devices are available upon request. American Sign Language (ASL) Interpreters are available with at least three (3) business days notice before the meeting date.

MINUTES OF THE MEETING OF THE
OPERATIONS OVERSIGHT COMMITTEE
and
BOARD OF RETIREMENT*

LOS ANGELES COUNTY EMPLOYEES RETIREMENT ASSOCIATION

GATEWAY PLAZA - 300 N. LAKE AVENUE, SUITE 810, PASADENA, CA 91101

THURSDAY, OCTOBER 12, 2017, 11:50 A.M. – 11:55 A.M.

COMMITTEE MEMBERS

PRESENT: Alan Bernstein, Chair
Anthony Bravo, Vice Chair
Ronald Okum
Joseph Kelly
David Muir, Alternate

ALSO ATTENDING:

BOARD MEMBERS AT LARGE

Marvin Adams
Vivian H. Gray
Shawn R. Kehoe
Herman B. Santos
David Green, Chair, Board of Investments

STAFF, ADVISORS, PARTICIPANTS

Robert Hill
JJ Popowich

The meeting was called to order by Chair Bernstein at 11:50 a.m.

I. APPROVAL OF THE MINUTES

A. Approval of the minutes of the regular meeting of September 6, 2017

Mr. Kelly made a motion, Mr. Okum seconded, to approve the minutes of the regular meeting of September 6, 2017. The motion passed with Mr. Bernstein abstaining.

II. PUBLIC COMMENT

III. FOR INFORMATION

A. LACERA Operations Briefing
Robert Hill/JJ Popowich

Messrs. Hill and Popowich presented the monthly briefing on LACERA's operations. Many of the items highlighted may recur in subsequent briefings or may result in a future comprehensive OOC presentation.

- Public Records Request Update
- Report of Felony Forfeiture Cases Processed
- Beta Test – New Call Center After-Call Survey

IV. REPORT ON STAFF ACTION ITEMS

There was nothing to report on for staff action items.

V. GOOD OF THE ORDER

(For information purposes only)

VI. ADJOURNMENT

The meeting adjourned at 11:55 a.m.

***The Board of Retirement has adopted a policy permitting any member of the Board to attend a standing committee meeting open to the public. In the event five or more members of the Board of Retirement (including members appointed to the Committee) are in attendance, the meeting shall constitute a joint meeting of the Committee and the Board of Retirement. Members of the Board of Retirement who are not members of the Committee may attend and participate in a meeting of a Board Committee but may not vote on any matter discussed at the meeting. The only action the Committee may take at the meeting is approval of a recommendation to take further action at a subsequent meeting of the Board.**



October 23, 2017

TO: Operations Oversight Committee
Alan Bernstein, Chair
Anthony Bravo, Vice Chair
Joseph Kelly
Ronald Okum
David Muir, Alternate

FROM: James Beasley 
Administrative Services Analyst III

FOR: November 9, 2017 Operations Oversight Committee Meeting

SUBJECT: Cyber Liability Insurance

RECOMMENDATION

That your Committee recommends the Board of Retirement approve the purchase of Cyber Liability Insurance with the following insurance carrier:

Cyber Liability

- North American Specialty (NAS) Insurance
A.M. Best Rating: A+, XV
Limit: \$20 million
Premium: \$113,695

EXECUTIVE SUMMARY

For nearly two decades, LACERA has been purchasing various types of insurance coverage to mitigate the risk of unforeseen damages. A recognized gap in that coverage is Cyber Liability insurance. In response to data breaches and other cyber-crimes against organizations, LACERA continually evaluates ways to protect the Trust Funds against potential losses resulting from any such events.

In the last several years, data breaches have resulted in major fines and legal fees – not to mention administrative nightmares – for many companies, large and small. Many of these high-profile data breaches affected organizations like Yahoo, Sony,

Cyber Liability Insurance
Operations Oversight Committee
Page 2 of 5

Anthem, and the Federal Government. Businesses of all types are beginning to realize that no industry is safe from a data breach and having Cyber Liability Insurance can be an effective precaution to mitigate losses from such a breach.

Initially, Cyber Liability Insurance was targeted to e-commerce businesses. As non-e-commerce data breaches became more prevalent, Cyber Liability Insurance policies began to evolve. This evolution led to policies covering all types of organizations. Cyber Liability Insurance generally covers the financial liability for a data breach and cyber-crimes involving confidential customer information, such as Social Security numbers, credit card numbers, account numbers, driver's license numbers, and health records.

In light of the growing level of Cyber Security breaches and at your Boards' direction, LACERA has worked in conjunction with Kaercher, Campbell & Associates (KCAIB). LACERA contracts with KCAIB as our insurance Broker. Their purpose is to research appropriate insurance plans, conduct competitive bidding processes, and provide recommendations for LACERA's consideration. KCAIB provided a list of providers of Cyber Liability Insurance to LACERA. A cross-functional team evaluated each recommendation and analyzed the suitability of the coverage offered by each to determine which would provide the best coverage to protect the Trust Funds. This team took into account the organizational risks while considering both the cost benefits and the cost of the coverage.

CYBER LIABILITY INSURANCE

As with all computer-reliant entities, LACERA daily faces cyber and privacy threats. These threats include: malicious or negligent insiders, criminal hackers, third party compromise, and/or business interruption (cryptolocker/ransomware) types of attack to name a few. Due to our due diligence LACERA has been fortunate not to have experienced a data breach event of these types to date. Because we have no history to rely on, it is difficult to compile a realistic cost benefit analysis, and we have relied on industry statistics and figures to determine the possible financial impact to LACERA. Based on industry standards LACERA may be required to provide the following in an event of a data breach:

- Forensic Examination
- Notification of Third Parties
- Call Centers (to handle a higher volume of calls than we can support internally)

Cyber Liability Insurance
Operations Oversight Committee
Page 3 of 5

- Credit or Identity Monitoring
- Defense Cost
- Public Relations
- Regulatory Proceedings, Fines and Penalties
- Comprehensive Written Information Security Program

The costs and expenses of a data breach can be wide ranging. According to the 2016 NetDiligence Cyber Claims Study report, the average price tag associated with a data breach can cost the organization up to nearly \$15 million. They state that although each breach has its own set of unique factors, the financial impact is fairly consistent across the board. Depending on the severity of the breach, the impact to the organization may include any or all of the following:

- Information Loss
- Business Disruption
- Financial Loss
- Equipment Damages
- Defense Cost
- Loss of Members' Trust

SELECTION

Potential costs associated with a data breach can add up rapidly and can be a financial burden to the organization. The review team (team) that included representatives from the Administrative Services Division, Legal Office, Systems Division, and the Executive Office conducted an analysis to determine the appropriate amount of coverage required to ensure that LACERA is upholding its fiduciary responsibility in protecting the Trust Funds.

During this analysis, the team considered the size of the Trust Funds, the number of members (direct and indirect), the number of records (electronic and paper), and the scope of organizational losses due to breaches in organizations other than LACERA. The team determined that a \$20 million policy limit would be a sufficient amount of coverage to mitigate the severity of potential financial losses due to a data breach.

Based on LACERA's requirements, the Insurance Broker, KCAIB provided information from various insurance carriers who offer Cyber Liability Insurance. KCAIB is familiar with and aware of LACERA's process for selecting vendors; therefore, their focus was on obtaining the most comprehensive coverage at the most competitive price for

**Cyber Liability Insurance
Operations Oversight Committee
Page 4 of 5**

LACERA. KCAIB presented quotes from the following insurance carriers for consideration:

Carrier	A.M. Best Rating
NAS	A+, XV
XL – Indian Harbor	A+, XV
RSUI Indemnity Company	A+, XIII
Chubb	A++, XV
Hiscox Insurance Company	A, XI
Beazley Insurance Company	A, XII

The team conducted a comprehensive comparative analysis of each carrier’s quotation for the Cyber Liability Insurance to determine the policy that would provide the best protection of the Trust Funds while still opting for the most competitive price. The criteria used for this analysis is as follows:

- A side-by-side comparison of provisions
- The best protection of the LACERA Trust Funds
- The most comprehensive coverage for the most competitive price

After reviewing the results of the comparative analysis of each insurance carrier’s policy form, the team found the NAS Insurance Company’s (NAS) policy to be the most comprehensive. NAS was the only carrier to offer the full \$20 million policy limit. The other carriers offered \$5 million in coverage requiring multiple layers to reach the required \$20 million limit. This would amount to a 25 percent increase in cost over the NAS proposal.

NAS provides these services:

- Access to Expert Cyber Risk Advisors
- 24/7 Online Training Courses
- Sample Policies and Vendor Agreement Templates
- Cyber Security Training Courses
- Compliance Materials
- Risk Management Tools and Guidelines
- Anti-Phishing / Social Engineering courses
- Incident Response Plans

**Cyber Liability Insurance
Operations Oversight Committee
Page 5 of 5**

The proposal from NAS included hourly rates covered by the policy for pre-approved legal firms and forensic/data recovery specialists, should LACERA require these services in the event of a data breach. The team felt strongly that the fee coverage of \$250.00 per hour offered by NAS was lower than what the organization was willing to accept. As a result, NCAIB was effective in negotiating an increase to the hourly rate that would be more favorable to LACERA.

The newly negotiated hourly rates with NAS are as follows:

- Legal Fees - \$425.00 per hour
- Forensic/data Recovery Specialists - \$350.00 per hour

In addition to this hourly rate increase, NCAIB also requested on LACERA's behalf that NAS allow LACERA to select their choice of outside counsel to be added to the pre-approved list and NAS agreed. Therefore, NAS added the Alston and Bird Legal Firm to the pre-approved list for LACERA.

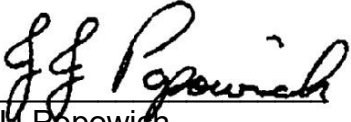
As an extra layer of review, the team also requested that Nossman L.L.P., LACERA's fiduciary counsel's expert in cyber insurance, review the coverage profile. Nossman advised that LACERA's proposed coverage is reasonable and at or above the coverage obtained by other public pension systems.

IT IS THEREFORE RECOMMENDED THAT YOUR COMMITTEE recommends the Board of Retirement approve the purchase of Cyber Liability Insurance with the following insurance carrier:

Cyber Liability

- North American Specialty (NAS) Insurance
A.M. Best Rating: A+, XV
Limit: \$20 million
Premium: \$113,695

Noted and Approved


JJ Popowich
Assistant Executive Officer

A decorative graphic on the left side of the slide, consisting of a network of light blue lines and circles that resemble a circuit board or data flow diagram. The lines are vertical and horizontal, with small circles at various points, creating a grid-like structure.

L.A. CERA

Los Angeles County Employees Retirement Association

CYBER LIABILITY

AGENDA

- History of Cyber Insurance
- Direct Risk To LACERA and Boards
- Legal Impacts
- What Is Covered
- Application Process
- Conclusion

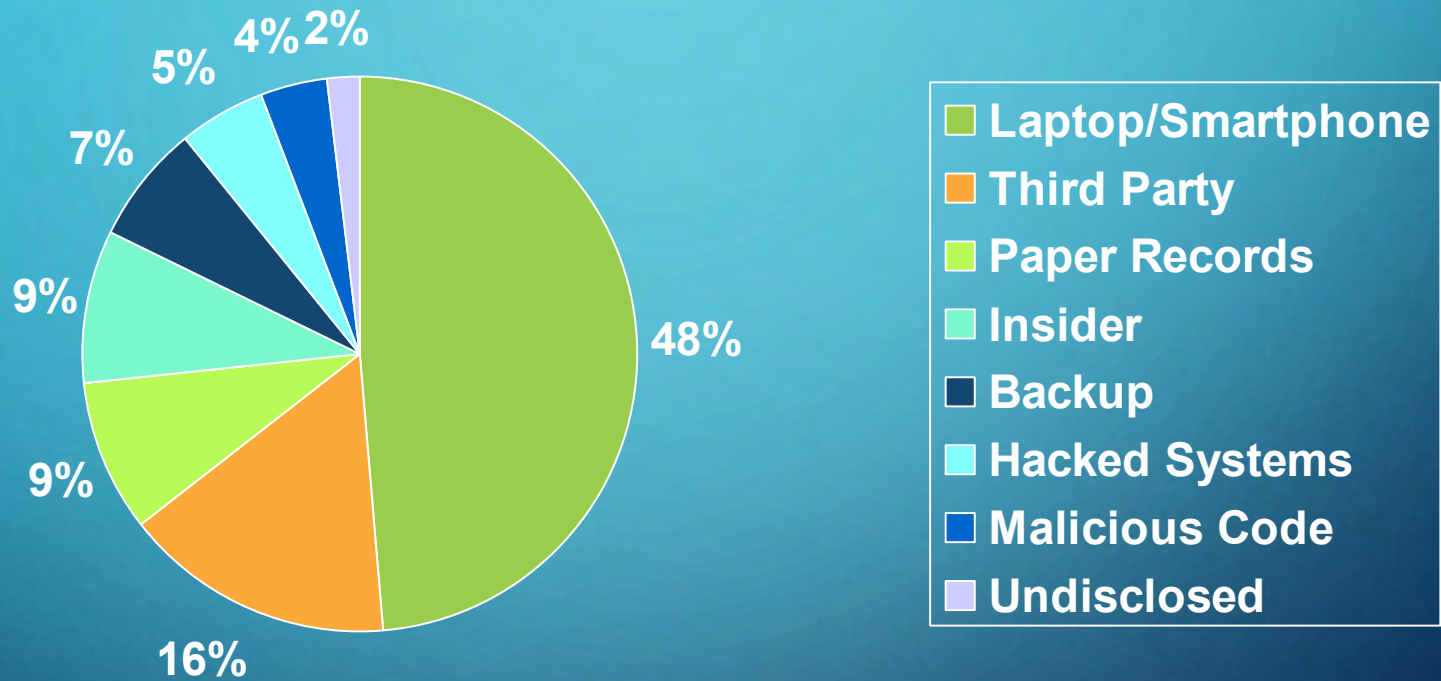
HISTORY OF CYBER LIABILITY

Originally developed in “dot.com” era for perceived risks of eCommerce and identified gaps in traditional insurance.

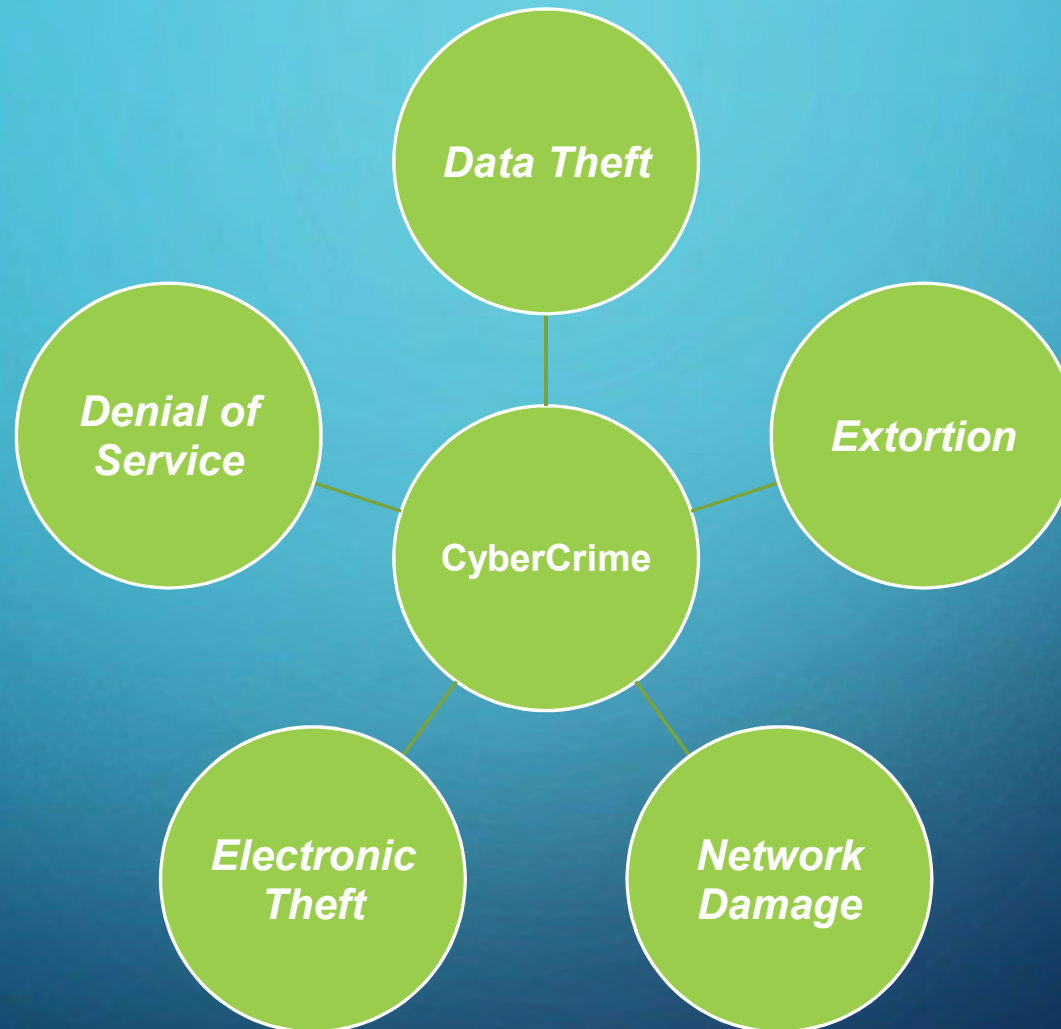
Early users included eCommerce companies, large financial institutions and technology service providers. Initial coverage limited to failure of computer security.

Significant expansion to the Cyber insurance product for “Privacy Liability” driven by the data breach notification and HIPPA laws.

SOURCES OF DATA BREACH



CYBER CRIME



COSTS OF DATA BREACH



**CYBER BREACHES
ARE EXPENSIVE**

COSTS

- Technical Forensics
- Theft Forensics
- Mailing Costs (notification to “class”)
- Call Center
- Credit Monitoring
- Loss Mitigation
- Attorney Expenses
- Defense Costs
- Settlement Costs
- Plaintiffs Fees

MORE COSTS

- Extra Expense
- Data Asset Loss
- Third-party damages for identity theft
- Reimbursement to credit card companies
- Replacement of damaged network
- Reward/Ransom expense
- Business revenue and expense due to compromised network
- Crisis management expense

LEGISLATION

- **California's Notice of Security Breach law (Cal. Civil Code §1798.29), enacted in 2002**
- California's laws changed effective January 1, 2012, requiring more information be contained in breach notification letters following a breach of personal information, including what happened, how it may affect the recipient of the letter, and how the recipient can protect themselves

LEGISLATION – CONTINUED

- California laws changed in 2015 regarding notification requirements . Companies will be required to notify the owner or licensee of personal information “immediately” after discovery of a breach of unencrypted personal information that was ,or is reasonably believed to have been, acquired by an unauthorized person.
- There is a requirement to notify the Attorney General when a breach affects over 500 people



DIRECTORS & OFFICERS IMPACT

FAILURE TO MAINTAIN PROPER
INSURANCE TO MITIGATE LOSS
COSTS

Insurance Coverage	Crime/Bond	General Liability	Kidnap and Ransom	Professional Liability	Property Business Interruption	Cyber
First Party Cyber Losses						
Network Interruption due to						
Computer Crime	█					█
Employee Sabotage	█					█
Operational Errors and Administrative Mistakes						█
Cyber Terrorism						█
Restoration, Recollection, Recreation of Digital Assets due to						
Computer Crime	█					█
Employee Sabotage	█					█
Operational Errors and Administrative Mistakes						█
Accidental Damage to Hardware						█
Cyber Extortion			█			█
Data Privacy and Security Third Party Losses						
Breach of Sensitive Third Party Information	█			█		█
Data Breach Caused by a Third Party Outsource				█		█
Corruption of Third Party Data by Malicious Code				█		█
Denial of Service or Malicious Code Delivered via your network				█		█
Corruption or Deletion of Third Party Data				█		█
Lost/Stolen Laptop or Hardware With Sensitive Third Party Data				█		█
Intellectual Property Infringement Plagiarism and Defamation		█		█		█
Data Privacy and Security First Party Losses						
Data Protection Fines and Penalties						█
Data Protection Investigation and Defense Expenses						█
Public Relations Costs						█
Data Protection Legal Expenses						█
Data Breach Notification Expenses						█
Credit/Identity Theft Monitoring Expenses						█

No Coverage

Possible Coverage

Coverage Provided

COVERAGE GAPS – OTHER INSURANCE

Type of Coverage	Why it does not apply to data breach
General Liability	GL policies cover bodily and property damage claims, not stolen identities.
Property	Property policies do not consider data as tangible property and does not cover identity information.
Crime or Employee Dishonesty	Crime insurance covers the theft of money, securities and property by employees. Identity information is not money or property. There is also no coverage for notification, credit monitoring or other liability arising from a data breach.
Public Officials or other Professional Liability	Public Officials and Professional policies respond to demands for damages. It is possible that some policies are written broadly enough to address a claim alleging an error in safeguarding information or invasion of privacy. The claim can only be submitted once sued, prior to being sued forensics, legal costs, notification and credit monitoring are the responsibility of the entity.

INSURED ORGANIZATION AND INSURED INDIVIDUALS

- Named Insured including subsidiaries
- Insured Individuals
 - Directors, officers, and managers
 - Partners and principals
 - Employees
 - Former/Past insured persons
 - Estates, heirs, executors, administrators, legal representatives
 - Spouses
 - Independent contractors

LIMITS RETENTION

- Claims Made coverage form
- Retro active Date – date of first policy inception
- Per Claim Limit – for each of the various types of coverage afforded
- Annual Aggregate Limit – applies across all different coverage agreements in the policy
- Sublimits – apply per policy form
- Deductibles/Retentions – various available
- Defense costs inside the limit

WHAT IS COVERED

- Network Security – Covers your liability when hacker uses your computer net to inflict damage on others.
- Privacy Breach – Covers your liability when private information is disclosed
 - Notification Expenses – when data is lost, you must notify all potential victims in a short period of time
 - Credit Monitoring – policies will cover up to one year of credit monitoring services for those exposed
 - Credit or Identity Repair Services – covers one year of services to repair creditor restore a victim's identity resulting from actual identity theft
 - Computer and legal forensic expenses

COVERAGE – CONTINUED

- Crisis Management – Public relations consultant expenses to protect your reputation
- Security Liability – failure to prevent the entrance or spread of a virus/hacker attack
- Website Media Liability – covers libel, slander and copyright infringement from your website content

COVERAGE – CONTINUED

- Regulatory Defense and Expenses – where regulatory actions brought by state or federal agency to enforce privacy regulations, provides defense cost coverage and in some cases covers penalties where insurable
- Electronic Media – Will pick up where a GL policy's advertising injury stops for things like libel, slander and copyright infringement regarding your website content
- Cyberextortion – covers expenses and ransom if a hacker threatens to shut down your network or release private records

COVERAGE – CONTINUED

- **First Party Data Asset** – covers expense to recover data you have lost due to a computer virus or hacker attack
- **Coverage for the records stored in any format and in any location** – including paper records, digital records, records on laptops or other portable storage devices as well as your records stored by third parties
- **Coverage for the activities of rogue employees** – intentional acts by an employee

COVERAGES

Security and Privacy Liability (3rd party – requires a demand / litigation / investigation)

- A successful computer attack against an insured that causes harm to a third party
- A wrongful disclosure or breach of private/confidential data

Event Management (1st party – no 3rd party claim required)

- Breach Coach / Law Firm Consultation
- Forensic Investigation
- Legal Assistance to Determine Appropriate Response
- Notification Costs (print/mail letter)
- Call Center Services
- Identity Monitoring

ADDITIONAL COVERAGES

Media Content Liability (3rd Party)

- Protects insureds from intellectual property perils such as trademark infringement, copyright infringement, libel, slander, defamation, invasion of privacy and others
- Designed for all companies that are not publishers and broadcasters
- Covers both online and offline content

Cyber Extortion Insurance (1st Party)

Covers threats to commit a computer attack against an insured and a demand for money to terminate the threat

Network Business Interruption (1st Party)

Covers loss of profits and additional costs that would not have been incurred but for a network interruption

COVERAGE FEATURES

- Worldwide coverage
- Civil Liability
 - Defense Costs
 - Single/class action
 - Potential plaintiffs can include affected group, financial institutions, etc.
- Privacy/Security Regulation Actions (aggregate sublimit)
 - Defense Costs
 - Payment of civil fine or penalty
 - Regulatory compensatory award

COVERAGE FEATURES – CONTINUED

- Notification and Crisis Management Costs
 - Mailing costs
 - Offers of services to affected group (which may be voluntary) including credit reports, credit monitoring, credit protection, identity theft insurance, etc.
 - Computer forensics outside experts
 - Outside PR and legal advice
 - Professional call center
 - Others costs associated with credit card association rules

WHAT INFORMATION GOES INTO UNDERWRITING A CYBER LIABILITY POLICY

- Application
- Supporting Documents
 - IT security questionnaire
 - Third party security assessment
- Underwriters, carrier IT security consultant and applicant IT security officer conference call to discuss controls – if needed

HOW ITS RATED – FACTORS

- Network Security Measures
- Personnel, Policies and Procedures
- Information Security
- Type of Data Maintained
- Number of Individual Records
- Information Security Procedures
- Encryption and Storage
- Data Sharing and Outside Access
- Website and Content Information
- Website Type/Material
- Legal Procedures
- Extent of Contractual Risk Transfer
- Loss History
- Frequency Matters More Than Severity
- Prior Losses

CLAIM PROCESS

- Internal Response
 - Incident Response Plan
- Reporting to the Carrier
 - 24/7 Call Center Number
 - Claim Setup
 - Initial Response
- The Response
 - Breach Coach
 - Vendor Selection
 - Forensic Investigation
 - Notification Preparation & Execution
 - Call Center Services
 - Defense of a Suit or Regulatory
 - Investigation


CONCLUSION

- Data is a highly valuable asset.
- Significant risk exposures related to information security and privacy liability are not conclusively covered by traditional insurance.
- “Cyber” insurance policies are available with coverage, limits and premiums tailored to standard market enterprises.
- “Cyber” insurance is a viable method of risk transfer.

FOR INFORMATION ONLY

October 31, 2017

TO: Operations Oversight Committee
Alan Bernstein, Chair
Anthony Bravo, Vice Chair
Joseph Kelly
Ronald Okum
David Muir, Alternate

FROM: JJ Popowich, Assistant Executive Officer 
Bernie Buenaflor, Interim Assistant Executive Officer 

FOR: November 9, 2017 Operations Oversight Committee Meeting

SUBJECT: **LACERA OPERATIONS BRIEFING**

The purpose of this briefing is to share insights on staff activities, updates on goals, and discuss opportunities and/or concerns. Many of the items highlighted may recur in subsequent briefings or may result in a future comprehensive OOC presentation.

- Public Records Request Update
- Report of Felony Forfeiture Cases Processed

DATE RECEIVED	REQUESTER	DOCS REQUESTED
09-25-17	D. Kushner, Individual	<p>Requested copies of Quarterly Performance Reports presented to the Board of Investments for the period June 30, 2011 through June 30, 2017.</p> <p><i>Transmitted 25 documents.</i></p> <p><i>Sent 7 emails. One email for each year with the appropriate Quarterly Performance Reports attached.</i></p>
09-29-17	J. Clark, Individual	<p>Requested complete list of LACERA pension plan equity holdings for 2017.</p> <p><i>Transmitted 2 documents.</i></p> <p><i>US Equity Holdings as of June 30, 2017 and Non-US Equity Holdings as of June 30, 2017.</i></p>
10-02-17	R. Rao, Pageant Media	<p>Questions / comment regarding LACERA's new RFP for a U.S. and non-U.S. equity emerging manager:</p> <p>Material provided a few months ago states that the system plans to transition from fund-of-fund emerging managers (both of whom were terminated in August) to direct investment in global equity through emerging managers.</p> <p>Is this why the new RFP was issued? How big is the mandate for the chosen firm (in \$)?</p> <p>Since LACERA is trying to cut down the number of managers it has in this asset class, how many managers does it hope to have finally?</p> <p><i>The RFP is part of the implementation of the Board's long term goal as you stated. There is no specific size for the mandate, but it can be up to LACERA's asset allocation policy of 5%; the exact allocation will be a function of the quality of submissions and portfolio fit. The number of managers will also depend upon the quality of submissions. LACERA could accept none or multiple managers. The RFP provides the Board flexibility to determine the best course for implementation of its objectives and policies. The Board has not stated a specific number of managers that it will eventually have.</i></p>
10-05-17	R. Lampert, Pavilion Corp	<p>Requested copy of the Kreischer Miller report that was reported recently on the on-going validation of private equity fees.</p> <p><i>Transmitted 2 documents.</i></p> <p><i>Email response on October 5, 2017: One attachment is LACERA's cover memo for KM's presentation deck and the other is their presentation deck.</i></p> <p><i>Sent via email: BOI memo dated August 30, 2017, from Internal Audit Division re Private Equity Fee Recalculation Project and document titled Kreischer Miller Private Equity Fee Recalculation Project Summary, September 2017.</i></p>
10-06-17	J. Peterson	<p>Requested board meeting documents with the following agenda items for Board meeting of October 11, 2017: Introduction to real assets and OPEB Asset Allocation.</p> <p><i>Transmitted 2 documents.</i></p>

DATE RECEIVED	REQUESTER	DOCS REQUESTED
		<p><i>Sent via email: Board of Investments memo dated September 29, 2017 re Introduction to Real Assets and Board of Investments memo dated October 11, 2017 re OPEB Asset Allocation.</i></p>
10-06-17	S. Blake, IPREO	<p>Requested most recent and complete portfolio of pension fund. Requested the CUSIP (or other identifiers), Issuer Name, Coupon, Maturity, Par/Principal Value and Bond Value for each fixed income position held (internally or externally), as well as the CUSIP (or other identifiers), Issuer Name, Shares Held, and Value for each equity position held (internally or externally). Additionally, if any of your portfolio positions are managed externally, please provide the name of the external manager responsible for these assets, and indicate which positions they manage.</p> <p><i>Transmitted 3 documents.</i></p> <ol style="list-style-type: none"> 1. LACERA's fixed income holdings by manager as of September 29, 2017; 2. LACERA's U.S. equity holdings by manager as of June 30, 2017; and 3. LACERA's Non-U.S. equity holdings by manager as of June 30, 2017. 4.
10-11-17	D. Gregory, Public Plan IQ	<p>Request access to and a copy of Los Angeles County Employees Retirement Association information regarding the meetings shown below.</p> <ul style="list-style-type: none"> • October 11, 2017 Board of Investments Meeting: All investment related discussion materials • October 11, 2017 Corporate Governance Committee Meeting: All investment related discussion materials. • October 11, 2017 Fixed Income/Hedge Funds/ Commodities Committee Meeting: All investment related discussion materials. • October 11, 2017 DVD recording of the Board of Investments & All Committee Meetings. <p><i>Transmitted 3 documents.</i></p> <p><i>Sent via email the BOI, Corporate Governance and Fixed Income/Hedge Funds and Commodities Agenda Packages for the October 11, 2017 meetings. DVDs mailed to Ms. Gregory on October 16, 2017.</i></p>
10-11-17	R. Rao, Pageant Media	<p>Questions regarding BOI Investments meeting held on October 11, 2017,</p> <ol style="list-style-type: none"> 1. What was discussed in the "introduction to real assets?" 2. Was any decision made about StepStone Consulting Group after its review? Did StepStone have any new private equity recommendations? 3. What did the board discuss about Clarion Investors III? 4. Were any managers hired, terminated, put on the watch list or taken off the watch list? Who and why?

DATE RECEIVED	REQUESTER	DOCS REQUESTED
		<p>5. Give details about the 2018 Hedge Funds Annual Investment Plan. How it's different from the system's current plan in this asset class and how it will affect commitment in the asset class/with existing managers. Was the plan approved by the board?</p> <p>6. What were the consent items discussed by the fixed come/hedge funds committee?</p> <p><i>Transmitted 2 documents.</i></p> <p><i>Sent email response answers:</i></p> <ol style="list-style-type: none"> 1. Attached Board Memo. 2. Attached Board Memo; this was an information item, no action. 3. The Board approved up to a 50 million investment in Clarion Investors III. 4. No terminations or hires. 5. The Fixed Income/Hedge Fund/Commodities meeting was postponed due to lack of quorum. 6. There were no consent items. <p><i>Sent via email: BOI memo dated September 19, 2017 re Performance Review of Private Equity Consultant Stepstone Group and BOI memo dated September 19, 2017 re Introduction to Real Assets.</i></p>
10-12-17	R. Fellner, Transparent California	<p>Requested copy of LACERA's Employee Compensation Report for the 2016 year under the provisions of California Govt. Code §§ 6250 - 6270, the California Public Records Act.</p> <p>Most California agencies find it easiest to respond to this request by producing a copy of the State Controller's Office (SCO) report that includes employee names. Please provide a copy of the working report, or any other combination of records, that contains the compensation data found on the SCO report alongside employee names. Alternatively, please provide copies of any other reports or records that contain information responsive to the purpose of this request: employee name in conjunction with their compensation data.</p> <p><i>First response sent via email:</i> LACERA has requested the payroll data from the custodian, Los Angeles County. As soon as LACERA receives the files, we will extract the information that you have requested and provide you with the records. Since LACERA is not the custodian, we will require an extension of the 10-day statutory response requirement to both acquire and process the data. We anticipate to provide you the data by October 30, 2017.</p> <p><i>Transmitted 1 document.</i></p> <p><i>Sent via email on October 15, 2017: 2016 LACERA Employee Compensation Report</i></p>
10-12-17	S. Claussen	San Diego City Employees' Retirement System (SDCERS) have requested benchmarking information from other agencies regarding the disability retirement benefit.

DATE RECEIVED	REQUESTER	DOCS REQUESTED
		<p>Requested information is in bulleted text. Responsive information is in bold italicized text.</p> <p>In response to the benchmarking information, LACERA has the following responses shown in bold text:</p> <ul style="list-style-type: none"> • Average number of disability applications per year. <p><i>Five-year average for FY's 2012-2017 is 492 disability applications per fiscal year</i></p> <ul style="list-style-type: none"> • General percentage of applications that are approved/denied. <p><i>For same period of time and considering only completed applications (pending and closures excluded) 91% of the cases were approved. 9% were denied.</i></p> <ul style="list-style-type: none"> • Length of processing time from application to Board decision. <p><i>Average processing time = 14 months or 1.13 years.</i></p>

Overpayment & Forgery Receivables 6 Month Period Ended June 30, 2017

- . strategic partnership between:
 - enefits Division
 - ember services
- . financial & accounting services
- . legal office



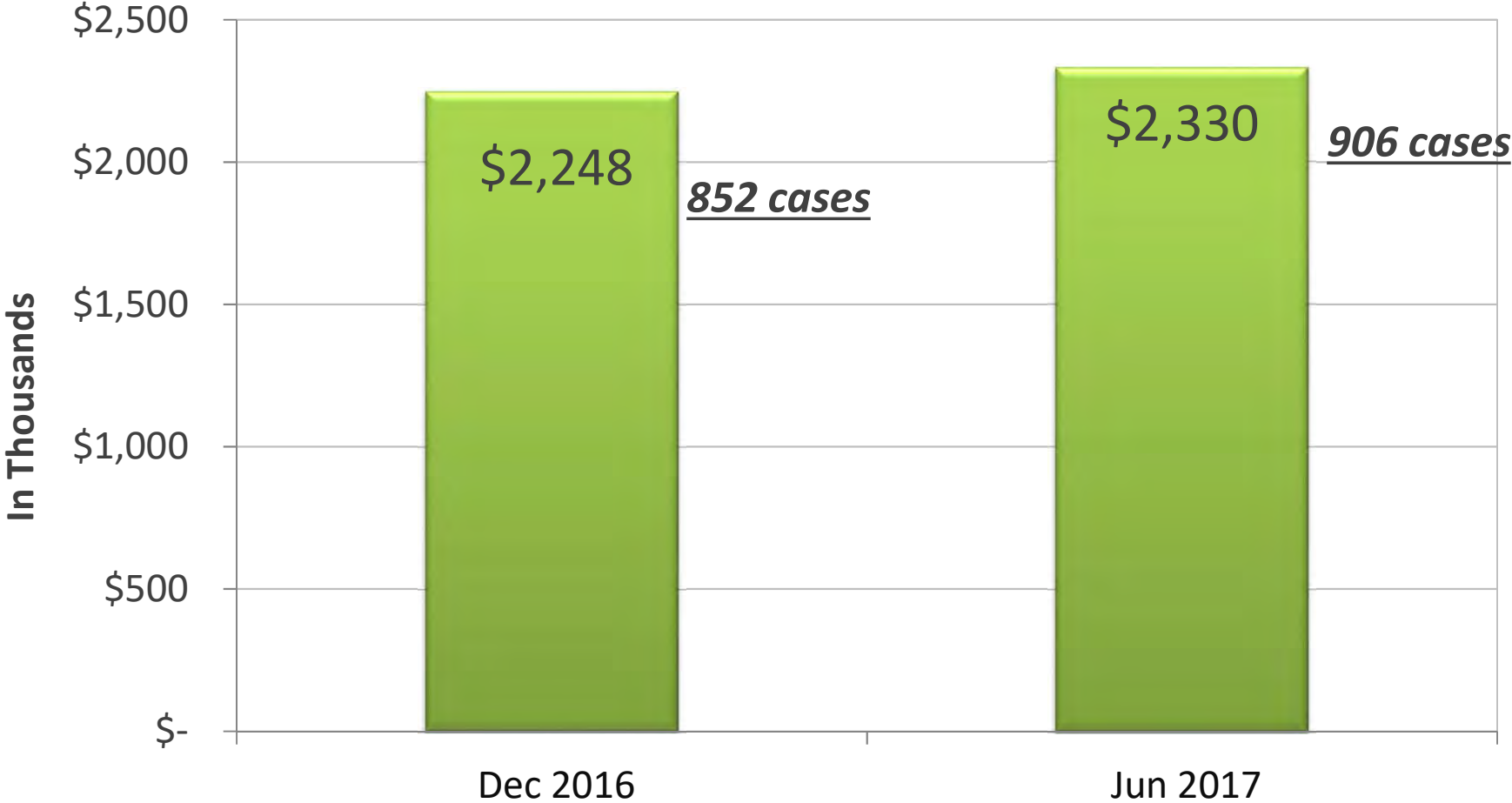
Presented by:

David Bayha – *Benefits Division*

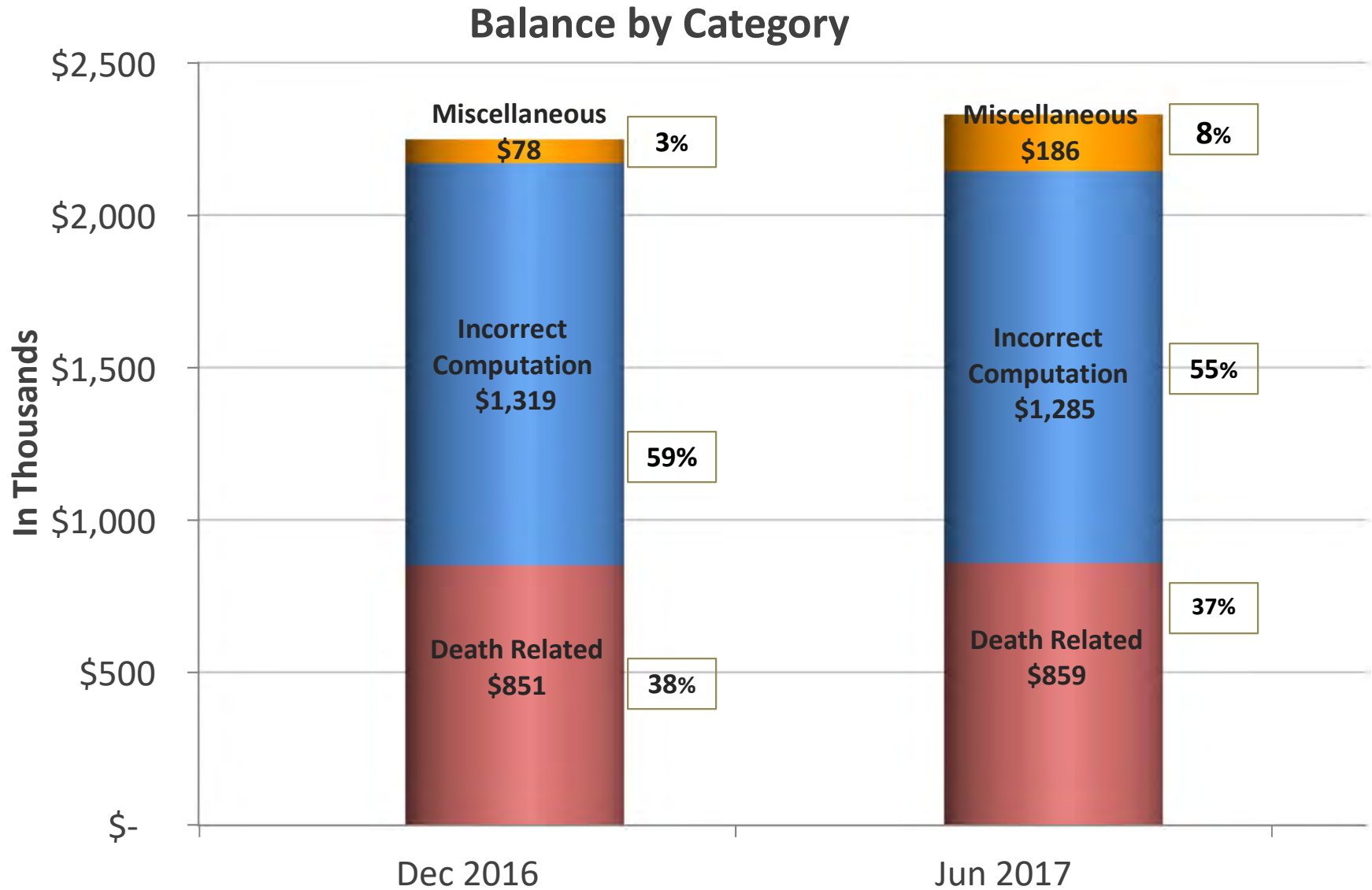
November 9, 2017

Overpayment & Forgery Receivables

Ending Balance Comparison

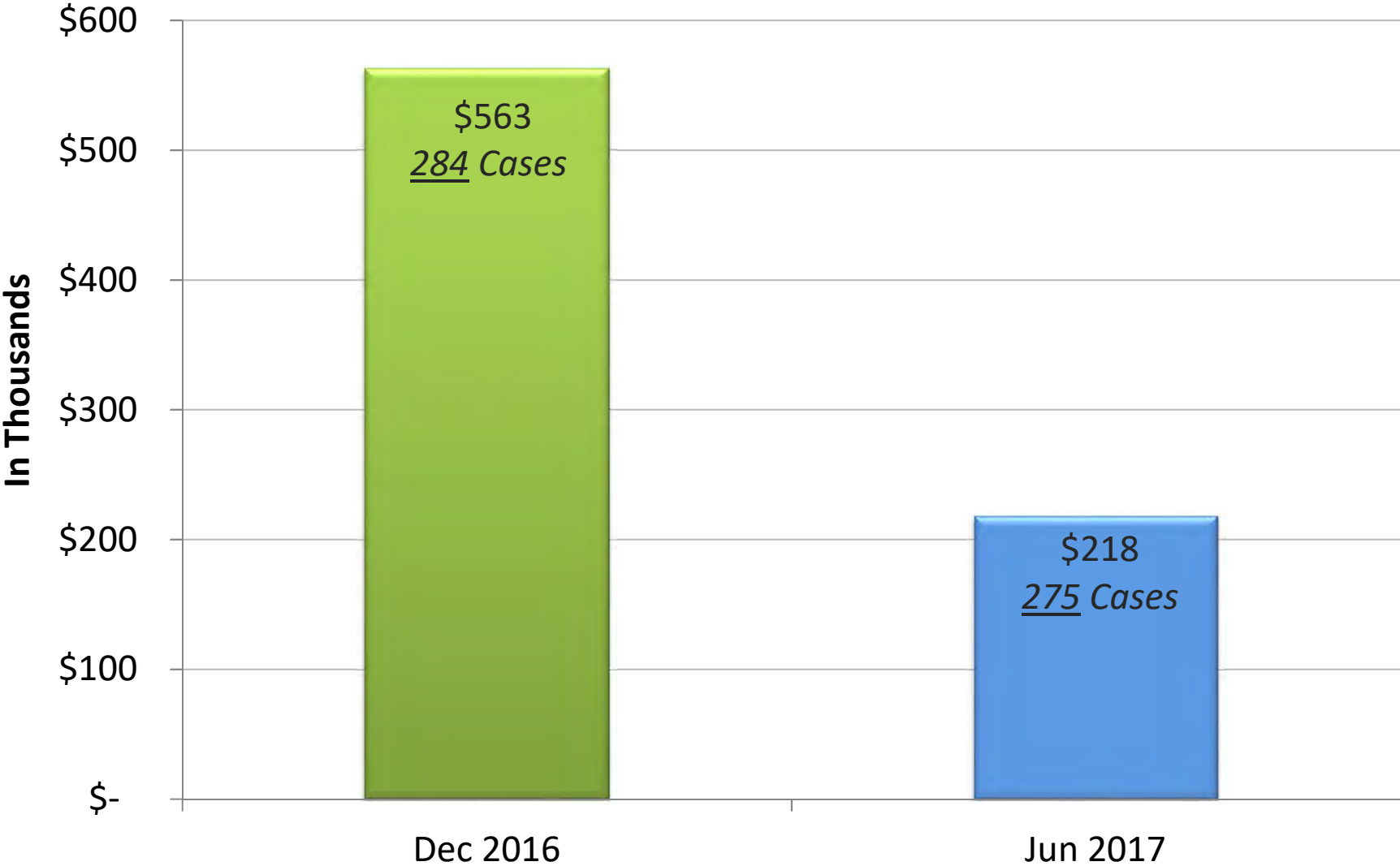


Overpayment & Forgery Receivables



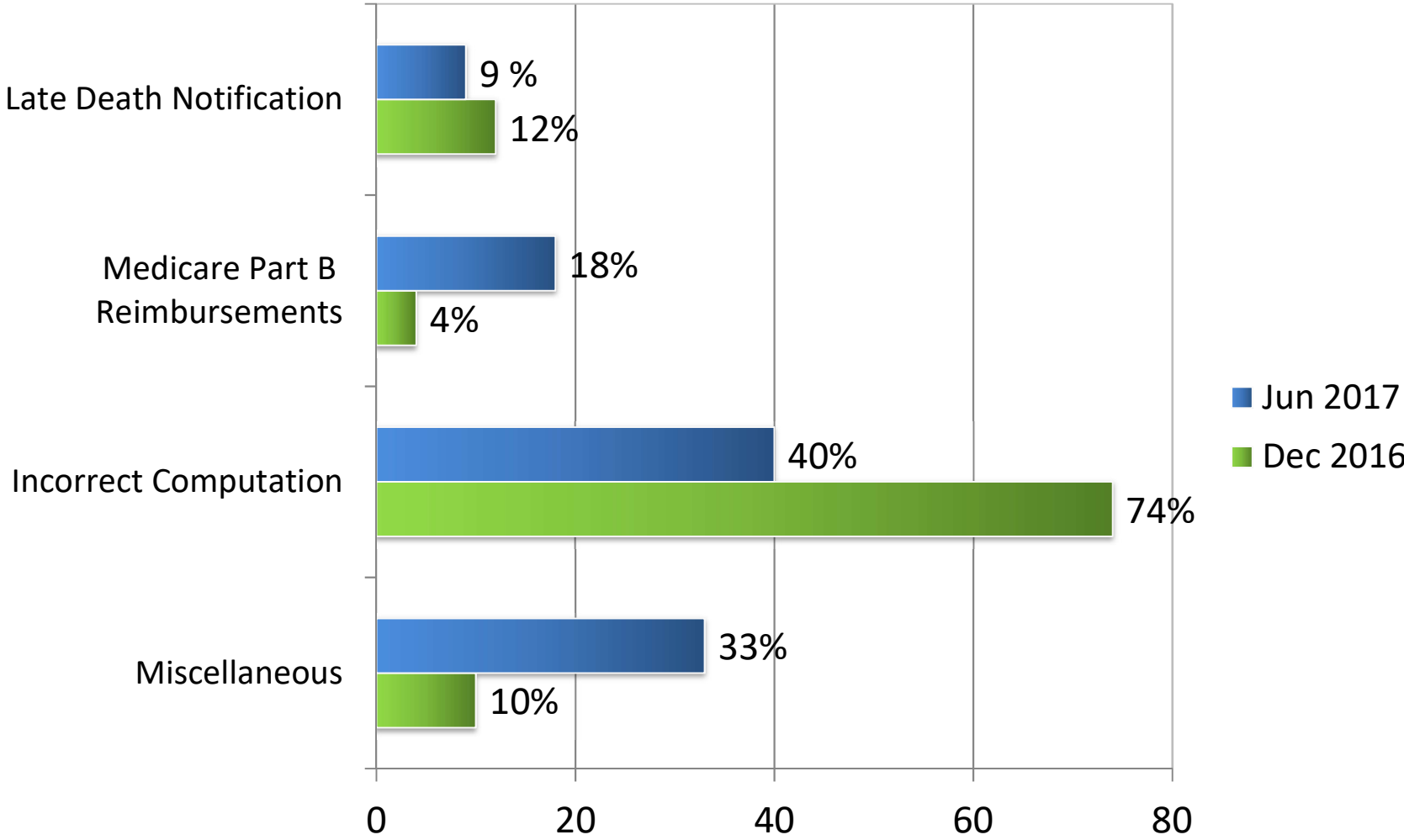
Overpayment & Forgery Receivables

New Cases Added Each Period Ended



Overpayment & Forgery Receivables

Breakdown of New Cases



Overpayment & Forgery Receivables

What have we been doing?

Medicare Part B Reimbursements

- 248 cases - \$40,011

Late Death Notification

- 6 cases - \$19,276

Incorrect Computation

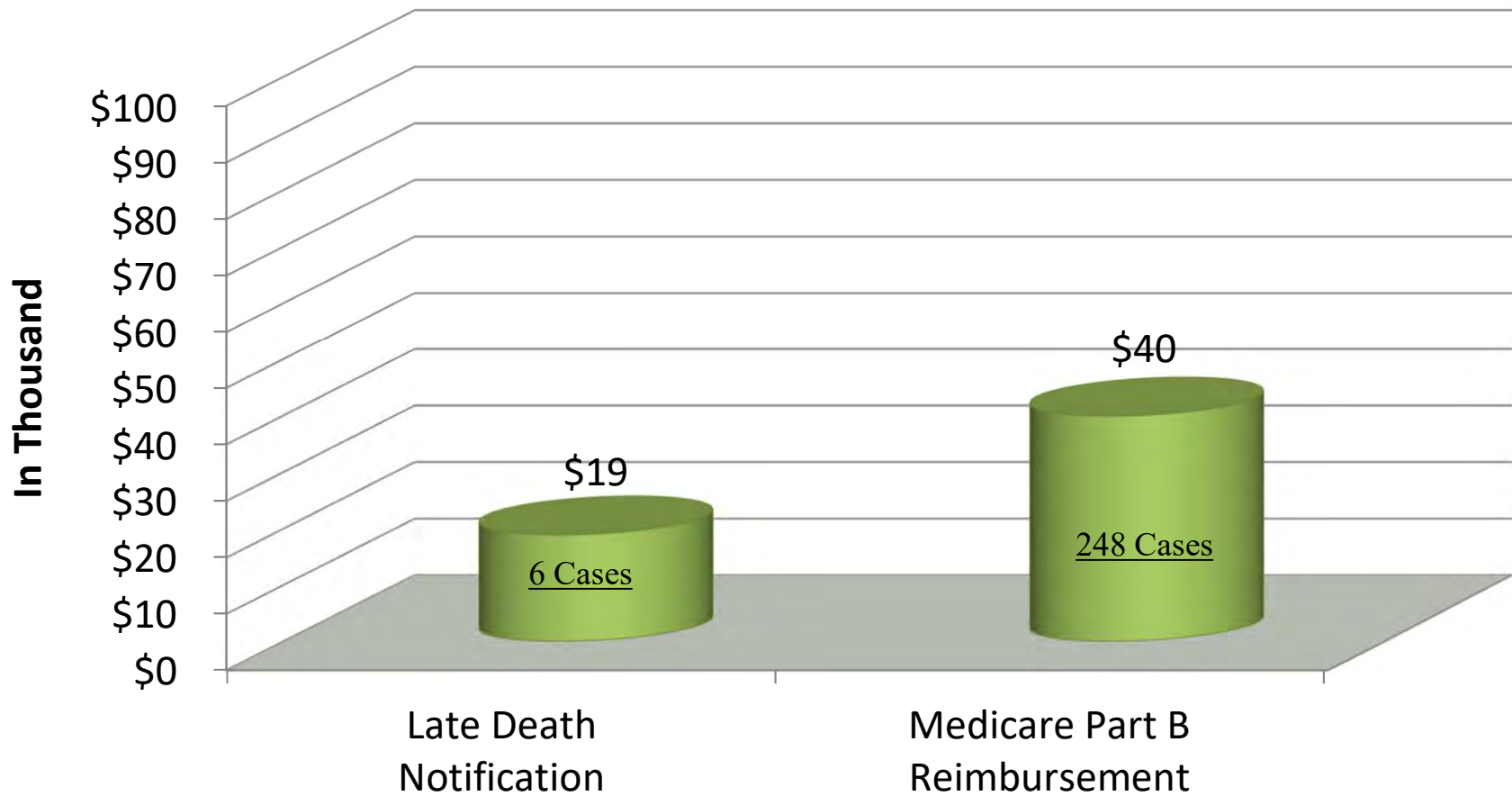
- 20 cases - \$87,229

Miscellaneous

- 1 cases - \$71,226

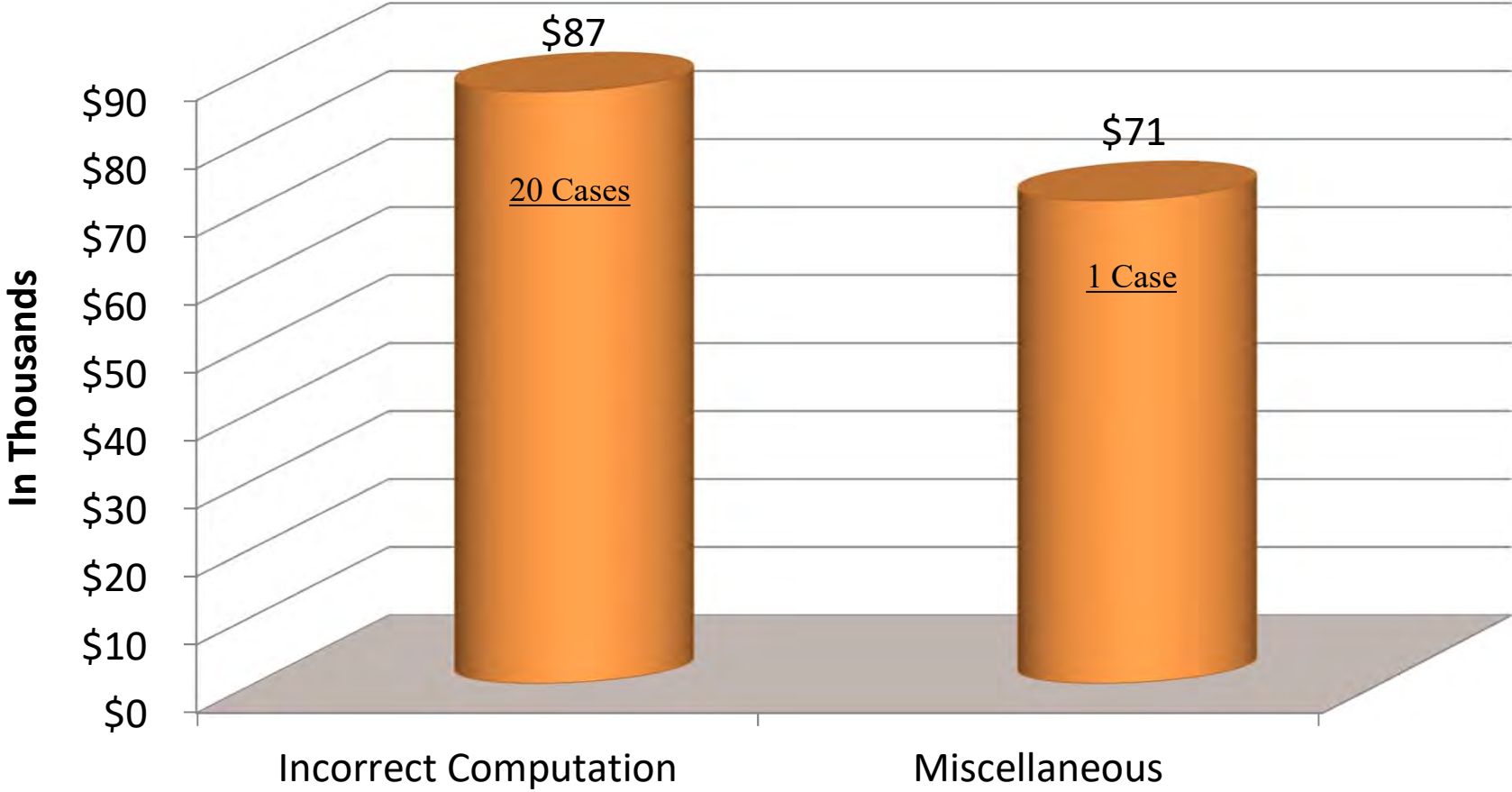
Overpayment & Forgery Receivables

New Cases – Beyond LACERA’s Control



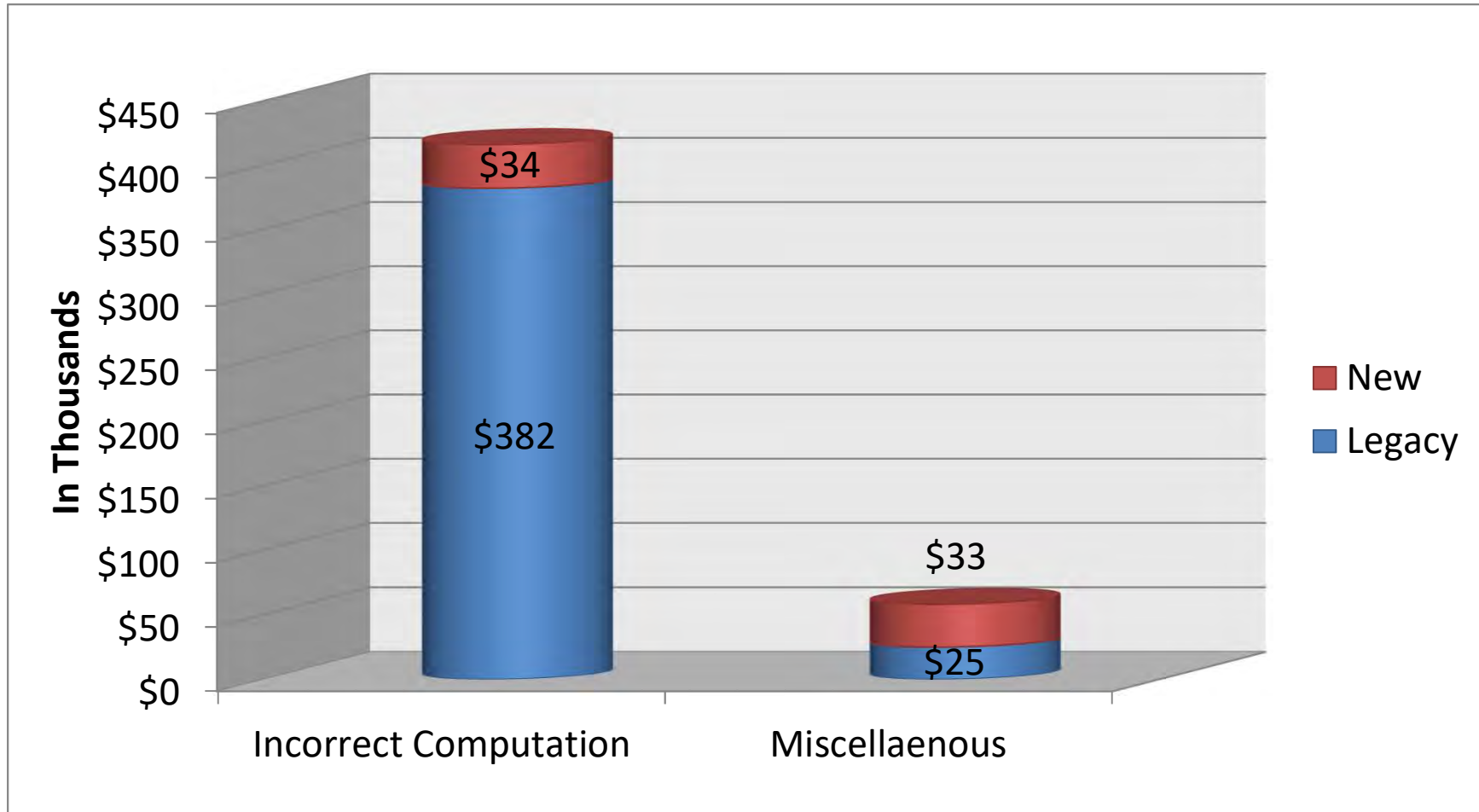
Overpayment & Forgery Receivables

New Cases – Within LACERA’s Control



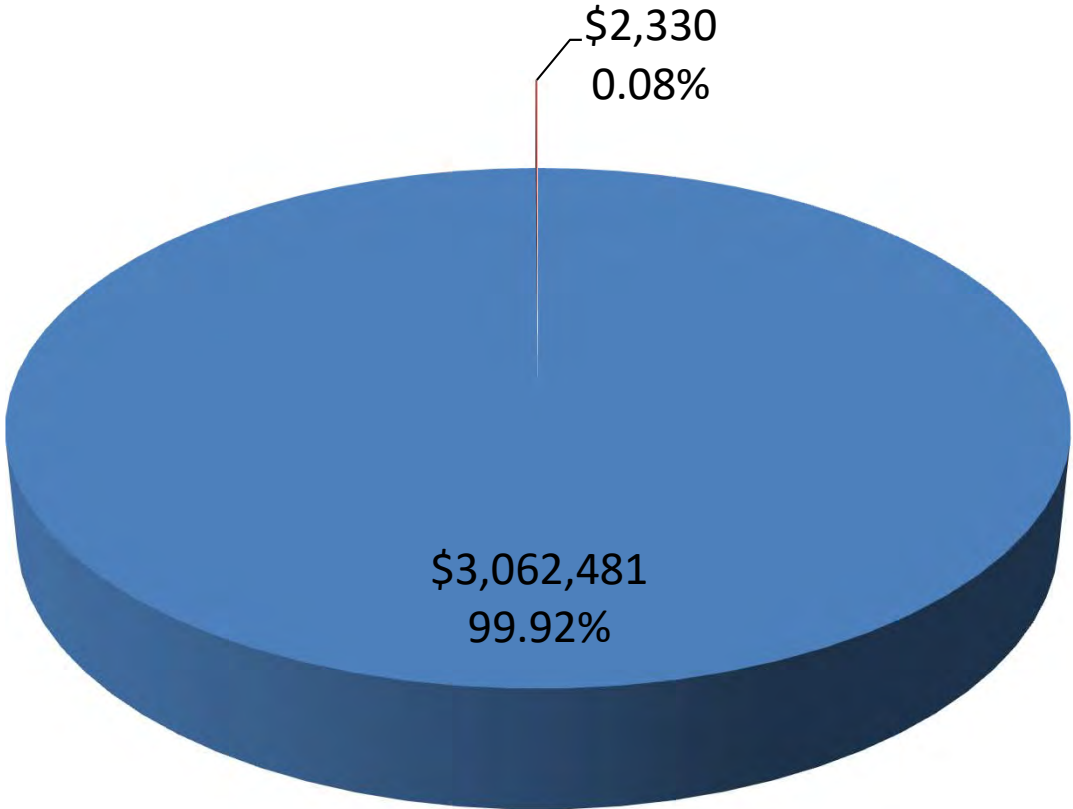
Overpayment & Forgery Receivables

New Cases – Within LACERA’s Control



Overpayment & Forgery Receivables

Balance as a Percentage of Payroll



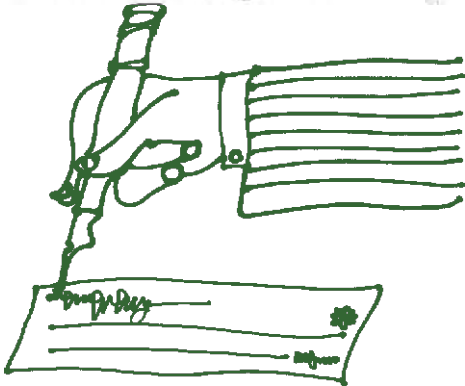
■ Payroll ■ Overpayment
(Dollars in Thousands)

Overpayment & Forgery Receivables

Collections for this Period



\$ 56,000 – Automatic Deduction/TTC



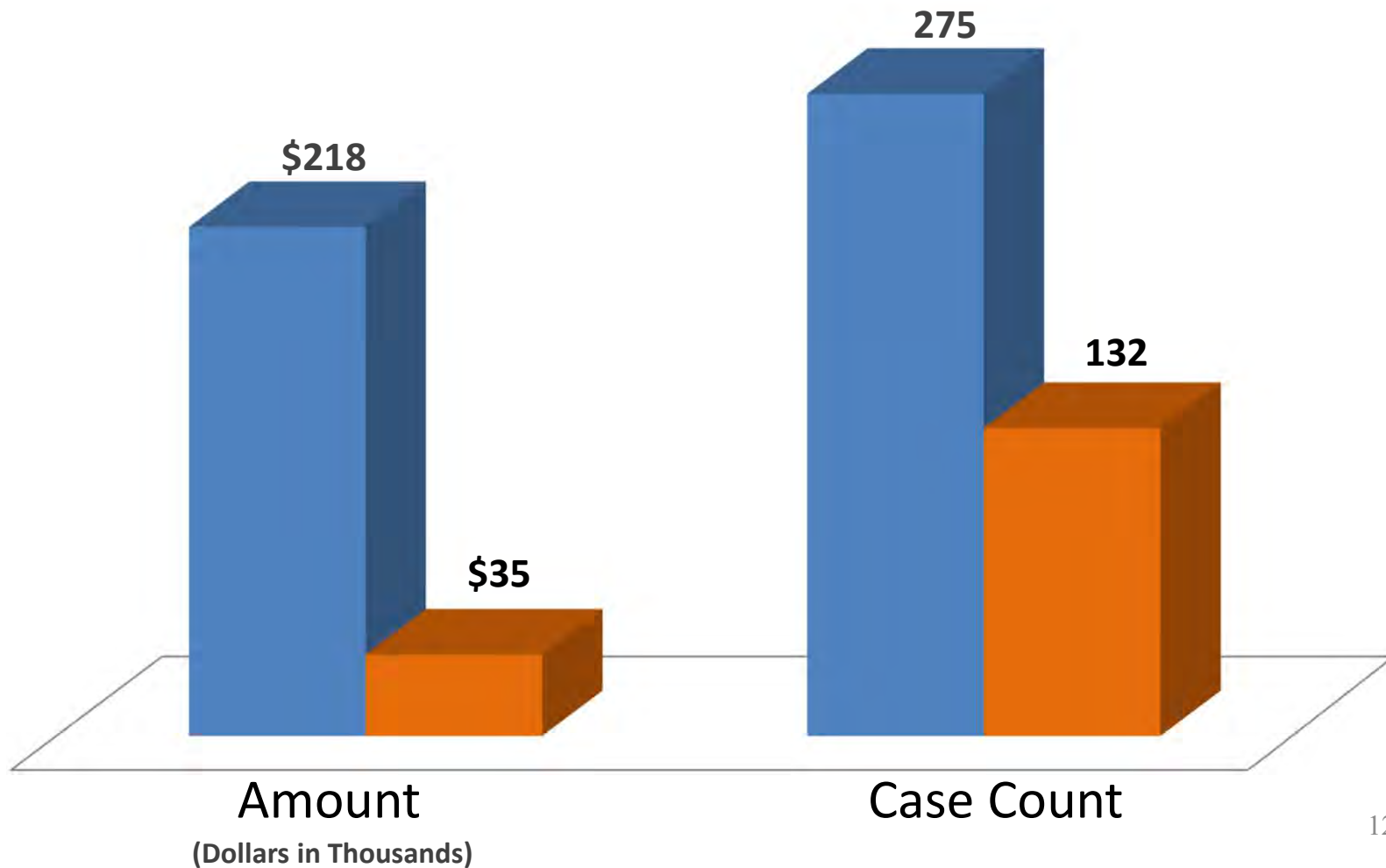
\$ 64,000 – Over the Counter Checks

\$ 120,000

Overpayment & Forgery Receivables

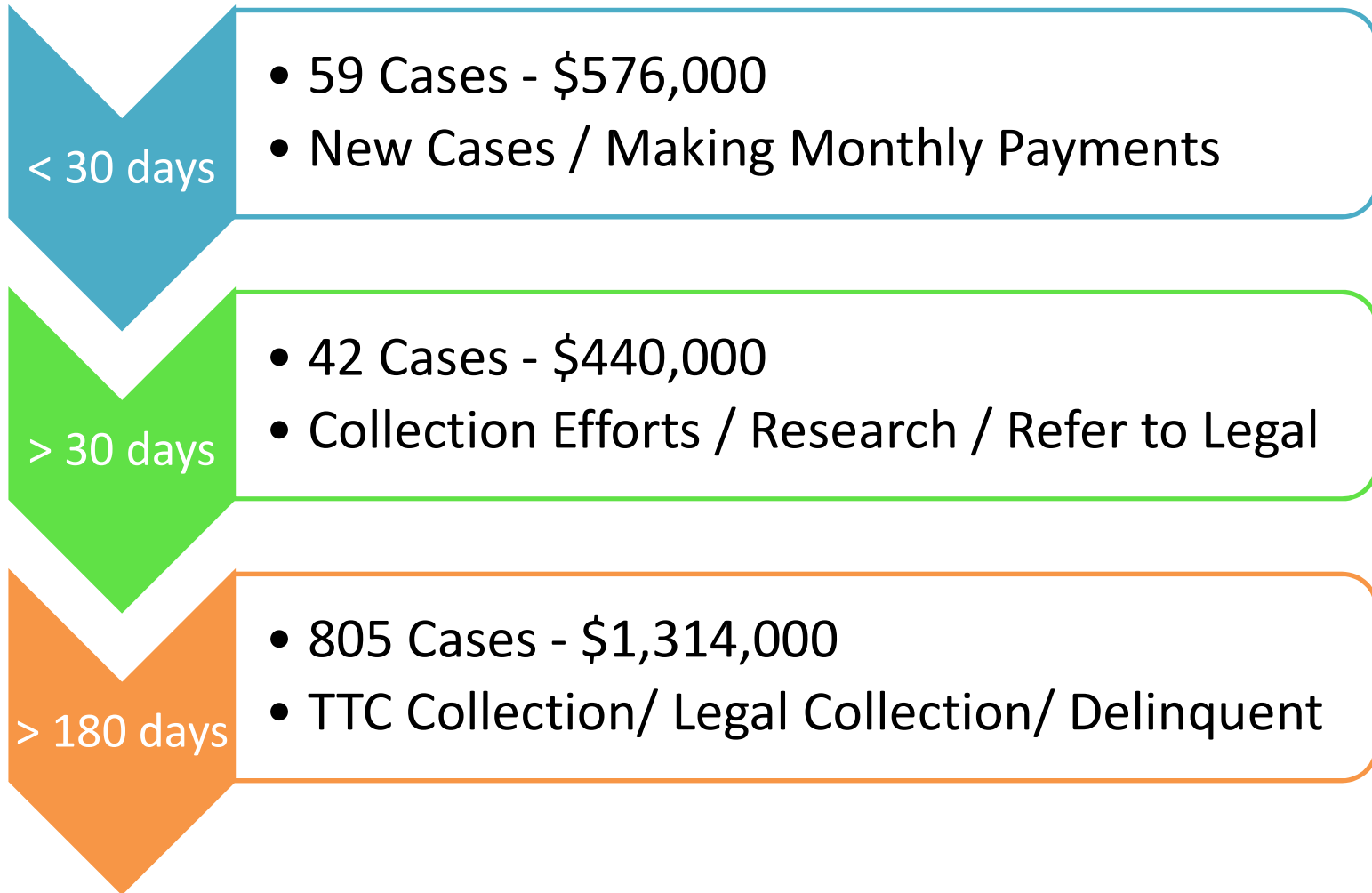
Collection Status: New Cases
For This Period

■ Set-up ■ Collected



Overpayment & Forgery Receivables

Aging Report



Overpayment & Forgery Receivables

Breakdown of Cases



Questions . . .

